Framework Schedule 6 (Order Form Template andCall-Off Schedules)

Order Form

CALL-OFF REFERENCE: K280021880

CALL-OFF TITLE: DVSA TTS CI and Legislative Change

CALL-OFF CONTRACT DESCRIPTION: The supplier is required to provide a scalable range of specialised IT resource as detailed in the buyer's specification in order to provide Continuous Improvement for DVSA's Theory Test Service systems. The supplier will also be required to deliver changes to DVSA's Theory Test systems in line with changes to Legislation as and when required

THE BUYER: Driver and Vehicle Standards Agency (DVSA)

BUYER ADDRESS 1 Unity Square, Queensbridge Rd, Nottingham

THE SUPPLIER: Kainos Software Ltd

SUPPLIER ADDRESS: Kainos House, 4-6 Upper Crescent,

Belfast, BT71NT

REGISTRATION NUMBER: NI019370

DUNS NUMBER: 232787408

SID4GOV ID: [Insert if known]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 31th March 2023.

It's issued under the Framework Contract with the reference number RM6263 for the provision of Digital Specialists and Programmes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement ofWork which shall be executed at the same time that the Call-Off Contract is executed,oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules).

An IR35 status determination will be applied for each and every SOW.

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

CALL-OFF LOT(S):
Lot 1 Digital Programmes

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict,the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. The buyer's full specification as detailed in the Further Competition document
3. The suppliers tender response
4. The cost schedules (SFIA rates and transition costs) completed by the supplier as part of their tender submission
5. Any volume discount provided by the supplier on the cost schedule document.
6. Joint Schedule 1 (Definitions) RM6263
7. Framework Special Terms
8. The following Schedules in equal order of precedence:

- Joint Schedules for RM6263
  - Joint Schedule 2 (Variation Form)
  - Joint Schedule 3 (Insurance Requirements)
  - Joint Schedule 4 (Commercially Sensitive Information)
  - Joint schedule 5 (Corporate Social Responsibility)
  - Joint schedule 6 (key subcontractors)
  - Joint schedule 7 (Financial difficulties)
  - Joint schedule 10 (Rectification Plan)
  - Joint schedule 11 (Processing data)
  - Joint schedule 13 (Cyber essentials scheme)

- Call-Off Schedules for RM6263
  - Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 3 (Continuous Improvement)
  - Call Off schedule 4 (Call Off tender)
  - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
  - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - [Call-Off Schedule 14B (Service Levels and Balanced Scorecard)]]
  - [Call-Off Schedule 15 (Call-Off Contract Management)]
  - Call-Off Schedule 18 (Background Checks)
  - Call-Off Schedule 20 (Call-Off Specification)
  - [Call-Off Schedule 25 (Ethical Walls Agreement)]

CCS Core Terms (version 3.0.11)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Redacted under FOIA Section 43, Commercial Interest

CALL-OFF START DATE:	31st March 2023
CALL-OFF EXPIRY DATE:	30th March 2025
CALL-OFF INITIAL PERIOD:	24 months
CALL-OFF OPTIONAL EXTENSION PERIOD:	12 months + 12 months
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	1 month
CALL-OFF CONTRACT VALUE:	Up to a maximum of £35,000,000.00
KEY SUB-CONTRACT PRICE:	[Insert the percentage of total projected Charges over Contract Period]

CALL-OFF DELIVERABLES
See details in Call-Off Schedule 20 (Call-Off Specification)]

BUYER's STANDARDS
From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards set out in Framework Schedule 1 (Specification). The Buyer requires the Supplier to comply with the following additional

Standards for this Call-Off Contract:
All standards specified within the Call Off specification (Schedule 20)

CYBER ESSENTIALS SCHEME
The Buyer requires the Supplier, in accordance with Joint Schedule 13 (Cyber Essentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £6,000,000.00 Estimated Charges in the first 12 Months of the Contract.

CALL-OFF CHARGES

Charging method for the delivery of core CI will be Time and Materials (T&M). The rate card detailed within Call-Off Schedule 5 (Pricing Details and Expenses Policy) will be used to calculate charges.

The rate card only applies should the T&M charging mechanism be used. Should an alternative charging mechanism be selected a price will be provided when the statement of work is being agreed.

In line with the Framework agreement the DVSA (the buyer) may consider and apply a different charging method to Statements of Work. Charging methods that may be considered are:

(1) Capped Time and Materials (CTM);
(2) Incremental Fixed Price;
(3) Time and Materials (T&M);
(4) Fixed Price; or
(5) A combination of two or more of the above Charging methods.

See details in Call-Off Schedule 5 (Pricing Details and Expenses Policy) for furtherdetails.]

The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law]

Where non-UK Supplier Staff (including Subcontractors) are used to provide any element of the Deliverables under this Call-Off Contract, the applicable rate card(s) shall be incorporated into Call-Off Schedule 5 (Pricing Details and Expenses Policy)and the Supplier shall, under each SOW, charge the Buyer a rate no greater than those set out in the applicable rate card for the Supplier Staff undertaking that element of work on the

Deliverables.

The relevant charging mechanism will be stipulated against each individual Statement of Work.

REIMBURSABLE EXPENSES

[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details andExpenses Policy)] [None]]

PAYMENT METHOD

Payment by BACS monthly in arrears.

BUYER'S INVOICE ADDRESS:

DVSA Accounts payable
DfT Shared Service Centre
5 Sandringham Park
Swansea Vale
Swansea
SA70EA

Alternatively electronic invoices can be issued to ssa.invoice@sharedservicesarvato.co.uk

BUYER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA Section 40, Personal Information

BUYER'S ENVIRONMENTAL POLICY
Not Applicable

BUYER'S SECURITY POLICY
The following DVSA Security Policies apply to this agreement (a copy of each policy is provided with this Order form):

Acceptable use policy
Access Control Policy
Clear desk and screen policy v3.0
DfT DPO Governance policy v3.0
DVSA Meetings recordings policy
DVSA COPE SyOps
DVSA Data Protection Policy
DVSA Security clearance for 3rd parties policy v0.3
DVSA IAP001 – Tier 0 ISMS Policy v1.0
DVSA IAP004 – SoA for DVSA
DVSA IAP102 – Tier 1 Information Assurance Policy
DVSA IAP202 – Tier 2 IA Policy for ICT Services
DVSA IA - Information Management Policy
DVSA IAP204 – Tier 2 Information Management Policy
DVSA IAP205 - Information Security Policy
DVSA IAP304 – Tier 3 Backup policy
DVSA IAP308 – Tier 3 Counter Terrorist Policy
DVSA IAP309 – Tier 3 Decommissioning Policy
DVSA IAP310 – Tier 3 Encryption data at rest and data in transit policy
DVSA IAP311 – Tier 3 Forensic readiness policy
DVSA IAP312 – Tier 3 IA Org policy
DVSA IAP314 – Tier 3 information transfer policy
DVSA IAP316 – Tier 3 Legal and contractual compliance policy
DVSA IAP317 – Tier 3 content malware and perimeter protection policy
DVSA IAP318 – Tier 3 Network security policy
DVSA IAP319 – Tier 3 patch management policy
DVSA IAP321 – Tier 3 personal security policy
DVSA IAP322 - Tier 3 physical security policy
DVSA IAP324 – Tier 3 removable media policy
DVSA IAP327 – Tier 3 operations security policy
DVSA IAP328 – Tier 3 security systems acquisition and development policy
DVSA IAP329 – Tier 3 security review policy
DVSA IAP330 – Tier 3 supplier security policy
DVSA IAP331 – Tier 3 vulnerability assessment and management policy

DVSA IAP332 – Tier 3 administrator conduct policy
DVSA IAP334 – Tier 3 Test data policy
DVSA IAP335 – Tier 3 wifi policy
IMS Audit policy
Incident management policy
Information assurance support statements
Information risk policy
Password and PIN policy
Protective monitoring policy

SUPPLIER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA Section 40, Personal Information

SUPPLIER'S CONTRACT MANAGER
Redacted under FOIA Section 40, Personal Information

PROGRESS REPORT FREQUENCY
On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY
Quarterly on the first Working Day of each quarter

KEY STAFF
Redacted under FOIA Section 40, Personal Information

Redacted under FOIA Section 40, Personal Information

KEY SUBCONTRACTOR(S)

Full Name	cloudThing Limited, trading as Kerv Digital
Registered Office Address	18 High Street, Longbridge, Birmingham, B31 2UQ
Type of Organisation	Limited Company
Company Registration Number	7510381
DUNS Number	217108519
VAT Number	152340739
Services to be provided	Specialist partner – Microsoft Dynamics

COMMERCIALLY SENSITIVE INFORMATION

Supplier confirmed as part of their bid:

Kainos considers that the following information provided in this document is exempt from disclosure under the Freedom of Information Act 2000 (FOI):

The CVs of staff qualify under the "Personal Information Exemption (s.40)" of the Freedom of Information Act and are exempt from disclosure under the Data Protection Act 1998. The Period for which this information should be confidential is the lifetime of the Data Subject.

Rate and pricing information is confidential and commercially sensitive and covered by the 'Commercial Interests' exemption (s.43) of the FOI, as the release of this information is likely to prejudice the commercial interests of Kainos and is likely to adversely affect its (and the Customer's) future negotiating position. The period that this information should be confidential for should be 5 years.

BALANCED SCORECARD

See Call-Off Schedule 14B (Service Levels and Balanced Scorecard)]

MATERIAL KPIs

The KPI's as detailed in Annexe A – KPI's apply to this contract

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables andperforming its obligations under the Call-Off Contract, that it will comply with the socialvalue commitments in Call-Off Schedule 4 (Call-Off Tender)

CUSTOMER RESPONSIBILITIES

Redacted under FOIA Section 43, Commercial Interest

STATEMENT OF WORKS

During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisionsdetailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:

Redacted under FOIA Section 40, Personal Information

For and on behalf of the Buyer:

Redacted under FOIA Section 40, Personal Information

Appendix 1

[**Insert** The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex1 to the Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)].

[**Insert** Each executed Statement of Work shall be inserted into this Appendix 1 in chronology.]

Annex 1 (Template Statement of Work)

1. STATEMENT OF WORK ("SOW") DETAILS	
Upon execution, this SOW forms part of the Call-Off Contract (reference below). The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverablesrequirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW. All SOWs must fall within the Specification and provisions of the Call-Off Contact. The details set out within this SOW apply only in relation to the Deliverables detailed herein and will notapply to any other SOWs executed or to be executed under this Call-Off Contract, unless otherwise agreed by the Parties in writing.	
Date of SOW:	
SOW Title:	
SOW Reference:	

Call-Off Contract Reference:	
Buyer:	
Supplier:	
SOW Start Date:	
SOW End Date:	
Duration of SOW:	
Key Personnel (Buyer)	
Key Personnel (Supplier)	
Subcontractors	

2. CALL-OFF CONTRACT SPECIFICATION - PROGRAMME CONTEXT	
SOW Deliverables Background	*[Insert details of which elements of the Deliverables this SOW will address].*
Delivery phase(s)	*[Insert item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta orLive].*
Overview of Requirement	*[Insert details including Release Types(s), for example, Adhoc, Inception, Calibrationor Delivery].*
Accountability Models	*Please tick the Accountability Model(s) that shall be used under this Statement ofWork:* *Sole Responsibility:☐* *Self Directed Team:☐* *Rainbow Team:☐*

3. BUYER REQUIREMENTS – SOW DELIVERABLES			
Outcome Description			
Milestone Ref	**Milestone Description**	**Acceptance Criteria**	**Due date**

MS01			
MS02			

Delivery Plan	
Dependencies	
Supplier Resource Plan	
Security Applicable to SOW:	The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance withParagraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security). **[**If different security requirements than those set out in Call-Off Schedule 9 (Security)apply under this SOW, these shall be detailed below and apply only to this SOW: *[insert if necessary]* **]**
Cyber Essentials Scheme	The Buyer requires the Supplier to have and maintain a Cyber Essentials PlusCertificate for the work undertaken under this SOW, in accordance with Joint Schedule 13 (Cyber Essentials Scheme).
SOW Standards	[Insert any specific Standards applicable to this SOW (check Annex 3 of Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules)]
Performance Management	[Insert details of Material KPIs that have a material impact on Contract performance] **Material KPIs** / **Target** / **Measured by** [Insert Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels andBalanced Scorecard)]
Additional Requirements	**Annex 1 –** Where Annex 1 of Joint Schedule 11 (Processing Data) in the Call-Off Contract does not accurately reflect the data Processor / Controller arrangements applicable to this Statement of Work, the Parties shall comply with the revised Annex1 attached to this Statement of Work.
Key Supplier Staff	**Key Role** / **Key Staff** / **Contract Details** [Indicate: whether there is any requirement to issue a Status Determination Statement]

<table>
<tr><td>Worker Engagement Status</td><td>[Yes / No] [Insert details]</td></tr>
<tr><td>[SOW Reporting Requirements:]</td><td>[Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call-Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:
<table>
<tr><th>Ref.</th><th>Type of Information</th><th>Which Services does this requirement apply to?</th><th>Required regularity of Submission</th></tr>
<tr><td>1.</td><td colspan="3">[insert]</td></tr>
<tr><td>1.1</td><td>[insert]</td><td>[insert]</td><td>[insert]</td></tr>
</table>
]</td></tr>
</table>

<table>
<tr><td colspan="2">4. CHARGES</td></tr>
<tr><td>Call Off Contract Charges</td><td>The applicable charging method(s) for this SOW is:
[Capped Time and Materials]
[Incremental Fixed Price]
[Time and Materials]
[Fixed Price]
[2 or more of the above charging methods]
[Buyer to select as appropriate for this SOW]

The estimated maximum value of this SOW (irrespective of the selected chargingmethod) is £[Insert detail].

The Charges detailed in the financial model shall be invoiced in accordance with Clause4 of the Call-Off Contract.</td></tr>
<tr><td>Rate Cards Applicable</td><td>[Insert SOW applicable Supplier and Subcontractor rate cards from Call-Off Schedule 5(Pricing Details and Expenses Policy), including details of any discounts that will be applied to the work undertaken under this SOW.]</td></tr>
<tr><td>Financial Model</td><td>[Supplier to insert its financial model applicable to this SOW]</td></tr>
<tr><td>Reimbursable Expenses</td><td>[See Expenses Policy in Annex 1 to Call-Off Schedule 5 (Pricing Details and ExpensesPolicy)]
[Reimbursable Expenses are capped at [£[Insert] [OR [Insert] percent ([X]%) of theCharges payable under this Statement of Work.]
[None]
[Buyer to delete as appropriate for this SOW]</td></tr>
</table>

<table>
<tr><td>5. SIGNATURES AND APPROVALS</td></tr>
<tr><td>Agreement of this SOW
BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the</td></tr>
</table>

Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:		
For and on behalf of the Supplier	Name and title	
	Date Signature	
For and on behalf of the Buyer	Name and title	
	Date	
	Signature	

ANNEX 1

Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

[TEMPLATE ANNEX 1 OF JOINT SCHEDULE 11 (PROCESSING DATA BELOW]

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: Redacted under FOIA Section 43, Commercial Interest **The Supplier is Controller and the Relevant Authority is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation,the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:* • ***Not Applicable for this contract*** **The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of theData Protection Legislation in respect of:* • ***Not Applicable for this contract*** **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposesof the Data Protection Legislation in respect of:* • *Business contact details of Supplier Personnel for which the Supplier isthe Controller,* • *Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,*

Duration of the Processing	*[Clearly set out the duration of the Processing including dates]* Redacted under FOIA Section 43, Commercial Interest
Nature and purposesof the Processing	*[Please be as specific as possible, but make sure that you cover all intendedpurposes.* Redacted under FOIA Section 43, Commercial Interest *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]* Redacted under FOIA Section 43, Commercial Interest
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public,users of a particular website etc.]* Redacted under FOIA Section 43, Commercial Interest
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]* Redacted under FOIA Section 43, Commercial Interest

Commercial Section
Driver and Vehicle Standards Agency
The Ellipse
Padley Road
Swansea
SA18AN

Phone:
Fax:
Textphone:

Redacted under FOIA Section 40, Personal Information

Kainos Software Ltd

Your ref:
Our ref: K280021880
Date: 28th March 2023

Dear Redacted under FOIA Section 40, Personal Information

Acceptance of tender for DVSA TTS CI and Legislative Change – K280021880

1. On behalf of the Secretary of State for Transport, I accept your tender under the terms and conditions of the Digital Specialists and Programmes Framework (rm6263). This letter and the documents listed below form a binding contract between you and this Department:

   - The terms and conditions for Framework reference rm6263
   - The Department's Statement of Requirements
   - Pricing Schedule
   - Order Form (Framework Schedule 6)
   - All schedules and their associated documents as detailed on the Order form

2. This contract will start on 31st March 2023 and end on 30th March 2025.

3. The maximum value for this contract is £35,000,000.00 exclusive of Value Added Tax. This is subject to iterative approval and at the discretion of DVSA.

4. You must be in possession of a written purchase order (PO), before commencing any work, or supplying any goods, under this contract. The Purchase Order Number for this contract will be generated shortly. Invoices submitted to the Department **must also quote the PO number** and must be submitted as directed **in the PO to:**

[Accounts Payable,
Shared Services arvato,
5 Sandringham Park,
Swansea Vale,
Swansea SA7 0EA.]

Invoices received without the correct Purchase Order Number will be returned to you and will delay receipt of payment.

Please sign and return the Order form to me at your earliest convenience. If you have any queries please do not hesitate to contact me.

Yours sincerely,

Redacted under FOIA Section 40, Personal Information

by authority of the Secretary of State for Transport

Crown Commercial Service

Core Terms

1. Definitions used in the contract

Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.

2.2 CCS does not guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.

2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.

2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:

(a) make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules);
(b) create new Call-Off Schedules;
(c) exclude optional template Call-Off Schedules; and/or
(d) use Special Terms in the Order Form to add or change terms.

2.5 Each Call-Off Contract:

(a) is a separate Contract from the Framework Contract;
(b) is between a Supplier and a Buyer;
(c) includes Core Terms, Schedules and any other changes or items in the completed Order Form; and
(d) survives the termination of the Framework Contract.

2.6 Where the Supplier is approached by any Other Contracting Authority requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order.

2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

2.8 The Supplier will not be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

(a) verify the accuracy of the Due Diligence Information; or
(b) properly perform its own adequate checks.

2.9 CCS and the Buyer will not be liable for errors, omissions or misrepresentation of any information.

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

(a) that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one);
(b) to a professional standard;
(c) using reasonable skill and care;
(d) using Good Industry Practice;
(e) using its own policies, processes and internal quality control measures as long as they do not conflict with the Contract;
(f) on the dates agreed; and
(g) that comply with Law.

3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the

Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they do not conform with Clause 3. If the Supplier does not do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4. Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).

4.3 All Charges and the Management Charge:

(a) exclude VAT, which is payable on provision of a valid VAT invoice; and
(b) include all costs connected with the Supply of Deliverables.

4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid,

undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

(a) includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer;
(b) includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any); and
(c) does not include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge).

4.6 The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

4.7 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.8 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, CCS or the Buyer can publish the details of the late payment or non-payment.

4.9 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables, then CCS or the Buyer may require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items.

4.10 If CCS or the Buyer uses Clause 4.9 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

(a) neither CCS or the Buyer can terminate a Contract under Clause 10.4.1;
(b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability and Deduction under this Contract;
(c) the Supplier is entitled to additional time needed to make the Delivery; and
(d) the Supplier cannot suspend the ongoing supply of Deliverables.

5.2 Clause 5.1 only applies if the Supplier:

(a) gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware;
(b) demonstrates that the Supplier Non-Performance would not have occurred but for the Authority

Cause; and
(c) mitigated the impact of the Authority Cause.

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract:

(a) during the Contract Period;
(b) for 7 years after the End Date; and
(c) in accordance with UK GDPR,
including but not limited to the records and accounts stated in the definition of Audit in Joint Schedule 1.

6.3 The Relevant Authority or an Auditor can Audit the Supplier.

6.4 During an Audit, the Supplier must:

(a) allow the Relevant Authority or any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit; and
(b) provide information to the Relevant Authority or to the Auditor and reasonable co-operation at their request.

6.5 Where the Audit of the Supplier is carried out by an Auditor, the Auditor shall be entitled to share any information obtained during the Audit with the Relevant Authority.

6.6 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

(a) tell the Relevant Authority and give reasons;
(b) propose corrective action; and
(c) provide a deadline for completing the corrective action.

6.7 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

(a) the methodology of the review;
(b) the sampling techniques applied;
(c) details of any issues; and
(d) any remedial action taken.

6.8 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

(a) be appropriately trained and qualified;
(b) be vetted using Good Industry Practice and the Security Policy; and
(c) comply with all conduct requirements when on the Buyer's Premises.

7.2 Where a Buyer decides one of the Supplier's Staff is not suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

(a) it has full capacity and authority to enter into and to perform each Contract;
(b) each Contract is executed by its authorised representative;
(c) it is a legally valid and existing organisation incorporated in the place it was formed;
(d) there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract;
(e) it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract;
(f) it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract;
(g) it is not impacted by an Insolvency Event; and
(h) it will comply with each Call-Off Contract.

8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:

(a) wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract; and
(b) non-payment by the Supplier of any Tax or National Insurance.

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 The description of any provision of this Contract as a warranty does not prevent CCS or a Buyer from exercising any termination right that it may have for breach of that clause by the Supplier.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:

(a) receive and use the Deliverables; and
(b) make use of the deliverables provided by a Replacement Supplier.

9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.

9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

(a) obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR; or
(b) replace or modify the relevant item with substitutes that do not infringe IPR without adversely affecting the functionality or performance of the Deliverables.

9.7 In spite of any other provisions of a Contract and for the avoidance of doubt, award of a Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing, with reference to the acts authorised and the specific IPR involved.

10. Ending the contract or any subcontract

10.1 Contract Period

10.1.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.1.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.2 Ending the contract without a reason

10.2.1 CCS has the right to terminate the Framework Contract at any time without reason by giving the Supplier at least 30 days' notice.

10.2.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason by giving the Supplier not less than 90 days' written notice.

10.3 Rectification plan process

10.3.1 If there is a Default, the Relevant Authority may, without limiting its other rights, request that the Supplier provide a Rectification Plan, within 10 working days .

10.3.2 When the Relevant Authority receives a requested Rectification Plan it can either:

(a) reject the Rectification Plan or revised Rectification Plan, giving reasons; or
(b) accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties.

10.3.3 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

(a) must give reasonable grounds for its decision; and
(b) may request that the Supplier provides a revised Rectification Plan within 5 Working Days.

10.3.4 If the Relevant Authority rejects any Rectification Plan, including any revised Rectification Plan, the Relevant Authority does not have to request a revised Rectification Plan before exercising its right to terminate its Contract under Clause 10.4.3(a).

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

(a) there is a Supplier Insolvency Event;
(b) there is a Default that is not corrected in line with an accepted Rectification Plan;
(c) the Supplier does not provide a Rectification Plan within 10 days of the request;
(d) there is any material Default of the Contract;
(e) there is any material Default of any Joint Controller Agreement relating to any Contract;

(f) there is a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract;
(g) there is a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management);
(h) there is a Change of Control of the Supplier which is not pre-approved by the Relevant Authority in writing;
(i) if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded; or
(j) the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them.

10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If any of the following non-fault based events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

(a) the Relevant Authority rejects a Rectification Plan;
(b) there is a Variation which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes);
(c) if there is a declaration of ineffectiveness in respect of any Variation; or
(d) the events in 73 (1) (a) of the Regulations happen.

10.5 When the supplier can end the contract

The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate a Call-Off Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6 What happens if the contract ends

10.6.1 Where a Party terminates a Contract under any of Clauses 10.2.1, 10.2.2, 10.4.1, 10.4.2, 10.4.3, 10.5 or 20.2 or a Contract expires all of the following apply:

(a) The Buyer's payment obligations under the terminated Contract stop immediately.
(b) Accumulated rights of the Parties are not affected.
(c) The Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the End Date.
(d) The Supplier must promptly delete or return the Government Data except where required to retain copies by Law.
(e) The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.
(f) The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).

10.6.2 In addition to the consequences of termination listed in Clause 10.6.1, where the Relevant Authority

terminates a Contract under Clause 10.4.1 the Supplier is also responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.

10.6.3 In addition to the consequences of termination listed in Clause 10.6.1, if either the Relevant Authority terminates a Contract under Clause 10.2.1 or 10.2.2 or a Supplier terminates a Call-Off Contract under Clause 10.5:

(a) the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and
(b) the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated.

10.6.4 In addition to the consequences of termination listed in Clause 10.6.1, where a Party terminates under Clause 20.2 each Party must cover its own Losses.

10.6.5 The following Clauses survive the termination or expiry of each Contract: 3.2.10, 4.2, 6, 7.5, 9, 11, 12.2, 14, 15, 16, 17, 18, 31.3, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.7 Partially ending and suspending the contract

10.7.1 Where CCS has the right to terminate the Framework Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Call-Off Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Call-Off Contracts that have already been signed.

10.7.2 Where CCS has the right to terminate a Framework Contract it is entitled to terminate all or part of it.

10.7.3 Where the Buyer has the right to terminate a Call-Off Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.7.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.7.5 The Parties must agree any necessary Variation required by Clause 10.7 using the Variation Procedure, but the Supplier may not either:

(a) reject the Variation; or
(b) increase the Charges, except where the right to partial termination is under Clause 10.2.

10.7.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.7.

10.8 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

(a) there is a Change of Control of a Subcontractor which is not pre-approved by the Relevant Authority in writing;
(b) the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4; or
(c) a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority.

11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this Framework Contract (whether in tort, contract or otherwise) is no more than £1,000,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Call-Off Contract (whether in tort, contract or otherwise) is no more than the greater of £5 million or 150% of the Estimated Yearly Charges unless specified in the Call-Off Order Form.

11.3 No Party is liable to the other for:

(a) any indirect Losses; or
(b) Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

(a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
(b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;
(c) any liability that cannot be excluded or limited by Law;
(d) its obligation to pay the required Management Charge or Default Management Charge.

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3(b), 9.5, 31.3 or Call-Off Schedule 2 (Staff Transfer) of a Contract.

11.6 In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed the Data Protection Liability Cap.

11.7 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.8 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

(a) Deductions; and

(b) any items specified in Clauses 11.5 or 11.6.

11.9 If more than one Supplier is party to a Contract, each Supplier Party is jointly and severally liable for their obligations under that Contract.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

(a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
(b) restore the Government Data itself or using a third party.

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

14.8 The Supplier:

(a) must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request;
(b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
(c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
(d) securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it; and
(e) indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:

(a) keep all Confidential Information it receives confidential and secure;
(b) except as expressly set out in the Contract at Clauses 15.2 to 15.4 or elsewhere in the Contract, not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent; and
(c) immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

(a) where disclosure is required by applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Law, the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
(b) if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party;
(c) if the information was given to it by a third party without obligation of confidentiality;
(d) if the information was in the public domain at the time of the disclosure;
(e) if the information was independently developed without access to the Disclosing Party's Confidential Information;
(f) on a confidential basis, to its auditors;
(g) on a confidential basis, to its professional advisers on a need-to-know basis; or
(h) to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 In spite of Clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 In spite of Clause 15.1, CCS or the Buyer may disclose Confidential Information in any of the following cases:

(a) on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer;
(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to;
(c) if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
(d) where requested by Parliament; or
(e) under Clauses 4.7 and 16.

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within five (5) Working Days of the Buyer's request the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

(a) publish the Transparency Information;
(b) comply with any Freedom of Information Act (FOIA) request; and/or
(c) comply with any Environmental Information Regulations (EIR) request.

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision in its absolute discretion.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as

possible without affecting the rest of the Contract, whether it is valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act 1999 (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

(a) provides a Force Majeure Notice to the other Party; and
(b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Either Party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier cannot assign, novate or transfer a Contract or any part of a Contract without the Relevant Authority's written consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central Government Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

(a) their name;
(b) the scope of their appointment; and
(c) the duration of their appointment.

24. Changing the contract

24.1 Either Party can request a Variation which is only effective if agreed in writing and signed by both Parties.

24.2 The Supplier must provide an Impact Assessment either:

(a) with the Variation Form, where the Supplier requests the Variation; or
(b) within the time limits included in a Variation Form requested by CCS or the Buyer.

24.3 If the Variation cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

(a) agree that the Contract continues without the Variation; or
(b) terminate the affected Contract, unless in the case of a Call-Off Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them; or
(c) refer the Dispute to be resolved using Clause 34 (Resolving Disputes).

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the Framework Prices or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably practical. They must also say if they think any Variation is needed either to the Deliverables, Framework Prices or a Contract and provide evidence:

(a) that the Supplier has kept costs as low as possible, including in Subcontractor costs; and
(b) of how it has affected the Supplier's costs.

24.7 Any change in the Framework Prices or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

24.8 For 101(5) of the Regulations, if the Court declares any Variation ineffective, the Parties agree that their

mutual rights and obligations will be regulated by the terms of the Contract as they existed immediately prior to that Variation and as if the Parties had never entered into that Variation.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address in the Framework Award Form.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier's cost the Beneficiary must both:

(a) allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim; and
(b) give the Indemnifier reasonable assistance with the claim if requested.

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that does not damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

(a) the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money; or

(b) the amount the Indemnifier paid the Beneficiary for the Claim.

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

(a) commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2); or
(b) do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

27.2 The Supplier must during the Contract Period:

(a) create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same;
(b) keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request; and
(c) if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

(a) been investigated or prosecuted for an alleged Prohibited Act;
(b) been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;
(c) received a request or demand for any undue financial or other advantage of any kind related to a Contract; or
(d) suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act.

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.3 it must specify the:

(a) Prohibited Act;
(b) identity of the Party who it thinks has committed the Prohibited Act; and
(c) action it has decided to take.

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

(a) protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
(b) any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law.

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

(a) all applicable Law regarding health and safety; and
(b) the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier.

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any Tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor Tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

(a) the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant; and
(b) other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may

reasonably need.

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under a Call-Off Contract, the Supplier must both:

(a) comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
(b) indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

(a) the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
(b) the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
(c) the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements; and
(d) the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

(a) Law;
(b) Clause 12.1; or

(c) Clauses 27 to 32.

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

(a) determine the Dispute;
(b) grant interim remedies; and/or
(c) grant any other provisional or protective relief.

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any Disputes arising out of, or connected to it, are governed by English law.

Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;

1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

1.3.13 where a standard, policy or document is referred to by reference of a hyperlink, if that hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Relevant Authority and the Parties shall update the reference to a replacement hyperlink;

1.3.14 any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

(a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.15 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.16 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone if specified within the Buyer's acceptance testing procedure and **"Achieved"**, **"Achieving"** and **"Achievement"** shall be construed accordingly;
Additional nsurances"	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees ;
Affected Party"	the Party seeking to claim relief in respect of a Force Majeure Event;
Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

Annex”	extra information which supports a Schedule;
Approval"	the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly;
Audit"	the Relevant Authority’s right to: a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier’s and each Subcontractor’s compliance with the Contract and applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority’s internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
Auditor"	a) the Relevant Authority’s internal and external auditors; b) the Relevant Authority’s statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office;

	e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;
Authority"	CCS and each Buyer;
Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
Authorised User"	CCS' and Buyers' individual or group of individuals (including employees, consultants, contractors and agents) authorised by CCS and/or the Buyer to: a) access and use the Platform for the purposes set out in Framework Schedule 7 (Call-Off Award Procedure); and b) the rights granted under (a) shall apply unless and until that authorisation is revoked by CCS or the Buyer;
BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
Balanced corecard"	a tool for Call-Off Contract management activity, through measurement of a Supplier's performance against key performance indicator, which the Buyer and Supplier may agree at the Call-Off Contract Start Date;
Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
Buyer"	the relevant public sector purchaser identified as such in the Order Form;
Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
Buyer Authorised epresentative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
Buyer egistration rocess"	the process to be completed in accordance with Framework Schedule 7 (Call-Off Award Procedure) or as otherwise notified to the Buyer in writing by CCS, the completion of which shall result in a potential Buyer being registered as a "Buyer" within the Platform which will entitle the Buyer to undertake a Call-Off Procedure in accordance with Framework Schedule 7, as supported by the Platform;

Buyer's uidance"	guidance for Buyers on how to buy digital services using the Framework Contract, located at the CCS website: https://www.crowncommercial.gov.uk/agreements/RM6263 ;
Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
Call-Off Contract eriod"	the Contract Period in respect of the Call-Off Contract;
Call-Off Expiry ate"	the latter of: a) the scheduled date of the end of a Call-Off Contract as stated in the Order Form; or b) the date of completion of the last Deliverable due under the last Statement of Work under the Call-Off Contract;
Call-Off ncorporated erms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
Call-Off Initial eriod"	the Initial Period of a Call-Off Contract specified in the Order Form;
Call-Off Optional xtension Period"	such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form;
Call-Off rocedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure);
Call-Off Special erms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
Call-Off Start ate"	the date of start of a Call-Off Contract as stated in the Order Form;
Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
Cap"	the maximum amount to be paid by the Buyer under a Time and Materials mechanism for the delivery of an agreed scope;
Capped Time and aterials"	Time and Materials payable up to a specified Cap for delivery of the agreed scope of Deliverables;
CaM Tool"	the capability assessment matrix (CAM) is a downselect or multi-identifier functionality tool within the Platform to be used by Buyers to identify capable suppliers able to meet its Statement of Requirements by means of (a) ranking the suppliers, or (b) shortlisting the suppliers, which is comprised of Resource Profile, Service Capability, Location and Scalability as described in and a copy of the CaM Tool is in Annex C of Framework Schedule 7 (Call-Off Award Procedure);

CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
CCS Authorised epresentative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
Central overnment Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
Change of ontrol"	is: a) a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; or b) any instance where the Supplier demerges into 2 or more firms, merges with another firm, incorporated or otherwise changes its legal form;
Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form and, if applicable, each Statement of Work, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
Commercially ensitive nformation"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
Comparable upply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
Compliance fficer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;

Confidential nformation"	any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential;
Conflict of nterest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS, as the context requires;
Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: a) applicable Start Date; or b) the Effective Date, up to and including the applicable End Date;
Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
Control"	a) control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010; or b) any instance where the Supplier demerges into 2 or more firms, merges with another firm, incorporated or otherwise changes its legal form; and "**Controlled**" shall be construed accordingly;
Controller"	has the meaning given to it in the UK GDPR;
Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions;

	iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets; c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: i) Overhead; ii) financing or similar costs; iii) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise; iv) taxation; v) fines and penalties; vi) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
CRTPA"	the Contract Rights of Third Parties Act 1999;
Data Protection mpact ssessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;

Data Protection egislation"	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy;
Data Protection iability Cap"	the amount specified in the Framework Award Form;
Data Protection fficer"	has the meaning given to it in the UK GDPR;
Data Subject"	has the meaning given to it in the UK GDPR;
Data Subject ccess Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
Day Rate"	the Pricing Mechanism where the Supplier will invoice the Buyer for Supplier Staff providing Deliverables (or one or more of the elements of the Deliverables) based on a rate for no more than 7.5 Work Hours performed by the Supplier's Staff based on the applicable grade(s)set out in Annex 1 of Framework Schedule 3 (Framework Prices);
Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
Default anagement harge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly;
Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);

Dispute"	any claim, dispute or difference (whether contractual or non-contractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
Dispute esolution rocedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as: a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables b) is required by the Supplier in order to provide the Deliverables; and/or c) has been or shall be generated for the purpose of providing the Deliverables;
DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of Tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
DPA 2018"	the Data Protection Act 2018;
Due Diligence nformation"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
Effective Date"	the date on which the final Party has signed the Contract;
EIR"	the Environmental Information Regulations 2004;
Electronic nvoice"	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
Employment egulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;

End Date"	the earlier of: a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or b) if a Contract or Statement of Work is terminated before the date specified in (a) above, the date of termination of the Contract or Statement of Work (as the context dictates);
Environmental olicy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
Equality and uman Rights ommission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
Estimated Year 1 harges"	the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;
"Estimated Yearly Charges"	for the purposes of calculating each Party's annual liability under Clause 11.2: a) in the first Contract Year, the Estimated Year 1 Charges; or b) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or c) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;
"**Exempt Buyer**"	a public sector purchaser that is: a) eligible to use the Framework Contract; and b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of: i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848); v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and Council; or

	ix) Directive 2009/81/EC of the European Parliament and Council;
"**Exempt Call-off Contract**"	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
"**Exempt Procurement Amendments**"	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;
"Expenses Policy"	the Buyer's expenses policy as set out in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy);

Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise) and shall include, in the case of CCS, the website domain names www.crowncommercial.gov.uk and [Insert] regarding the Platform;
Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
Fixed Price"	the Pricing Mechanism where Charges are agreed at a set amount in relation to all work to be done under a Contract, Statement of Work, Deliverable(s) (or one or more element of the Deliverable(s)) including all materials and/or Milestones, no matter how much work is required to complete each Contract, Statement of Work, Deliverable(s) (or one or more element of the Deliverable(s)) within the agreed scope, and the total amount to be paid by the Buyer will not exceed the agreed fixed price;
FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
Force Majeure vent"	any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including: a) riots, civil commotion, war or armed conflict;

	b) acts of terrorism; c) acts of government, local government or regulatory bodies; d) fire, flood, storm or earthquake or other natural disaster, but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;
Force Majeure otice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
Framework Award orm"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
Framework ontract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service;
Framework ontract Period"	the period from the Framework Start Date until the End Date of the Framework Contract;
Framework Expiry ate"	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
Framework ncorporated erms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
Framework ptional Extension eriod"	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
Framework rice(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
Framework pecial Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
Framework Start ate"	the date of start of the Framework Contract as stated in the Framework Award Form;
Framework ender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
Further ompetition rocedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
General Anti-buse Rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions;

General Change n Law"	a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
Good Industry ractice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
Government ata"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: a) are supplied to the Supplier by or on behalf of the Authority; b) the Supplier is required to generate, process, store or transmit pursuant to a Contract; c) any Personal Data for which CCS or the Buyer is the Controller; or d) all Buyer Registration Process data submitted by Buyers into the Platform, including the full auditable history of any and all transactions and procedures conducted via the Platform;
Group of conomic perators"	a group of economic operators acting jointly and severally to provide the Deliverables, which shall include a consortium;
Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
Halifax Abuse rinciple"	the principle explained in the CJEU Case C-255/02 Halifax and others;
HMRC"	Her Majesty's Revenue and Customs;
Hourly Rate"	the Pricing Mechanism where the Supplier will invoice the Buyer for the work undertaken by Supplier Staff providing the Deliverables (or one or more of the elements of the Deliverables) under the Contract (and, if applicable, each SOW) based on the division of the applicable Supplier Staff Day Rate by no less than 7.5 being the applicable Work Day where the Supplier's Staff's the applicable Supplier Staff grade is set out in Annex 1 of Framework Schedule 3 (Framework Prices);

ICT Policy"	the Buyer's policy and any Platform policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
Impact ssessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
Implementation lan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
Incremental Fixed rice"	the Price Mechanism where the overall Statement of Work is based on Capped Time and Materials, but where the prices for individual Deliverables Increments are fixed prior to the work being undertaken. The Charges for the first Deliverable Increment or Deliverables Increments for the Statement of Work will be fixed, but the Charges for subsequent Deliverables Increments will be reviewed and refined prior to the execution of each subsequent Deliverables Increment within the same Statement of Work;
Indemnifier"	a Party from whom an indemnity is sought under this Contract;
Independent ontrol"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly;
Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
Information ommissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;

Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;
Insolvency Event"	with respect to any person, means: (a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or: (i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; (b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person; (c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person; (d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days; (e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business; (f) where that person is a company, a LLP or a partnership: (i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person; (ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person; (iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

	(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or (g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;
Installation Works"	all works which the Supplier is to carry out at any time during the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract and, if applicable, each SOW;
Intellectual roperty Rights" r "IPR"	a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights having equivalent or similar effect in any country or jurisdiction and the right to sue for passing off;
Invoicing ddress"	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
IPR Claim"	any action, suit, claim, demand, Loss or other liability which the Relevant Authority or Central Government Body may suffer or incur as a result of any claim that the performance of the Deliverables infringes or allegedly infringes (including the defence of such infringement or alleged infringement or passing off) of any third party IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
IR35"	the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
Joint Controller greement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*);
Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
Joint Control"	where two or more Controllers agree jointly to determine the purposes and means of Processing Personal Data;
Key Staff"	the individuals (if any) identified as such in the Order Form and any Statement of Work;

Key Sub-ontract"	each Sub-Contract with a Key Subcontractor;
Key ubcontractor"	any Subcontractor: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract, and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;
Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
Location"	the place at or from which the Supplier's team will provide the Services under the Call-Off Contract and, if applicable, each SOW;
Losses"	all losses, liabilities, damages, costs, expenses (including legal and professional fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
Management harge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
Management nformation" or MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);
Material KPIs"	are Key Performance Indicators which are identified by the Buyer as having a material impact on the performance of the Call-Off Contract;

MI Default”	when two (2) MI Reports are not provided in any rolling six (6) Month period
MI Failure"	when an MI report: a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
MI Report"	a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
MI Reporting emplate"	the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
Milestone"	an event or task described in the Implementation Plan or Statement of Work;
Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
Misconduct”	has the meaning given to it in Paragraph 7.2 of Framework Schedule 7 (Call-Off Award Procedure);
Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
National nsurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier’s obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier’s Existing IPR;
Occasion of Tax on–Compliance"	where: a) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any Tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

	ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for Tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;
Off-Payroll Worker"	a worker (or contractor), not employed by the Supplier or any other organisation within the supply chain, that provides their services through their own private limited company or other type of intermediary which may include the worker's own personal service company, a partnership or an individual;
Open Book Data"	complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to: a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade; iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and

	h) the actual Costs profile for each Service Period;
Option”	the selection of an option by the Buyer which is incorporated into the Call-Off Contract and, if applicable, any Statement of Work, which the Supplier must comply with;
Optional xtension Period”	is the Buyer’s maximum optional extension period to the Call-Off Initial Period as set out in the Order Form;
Order"	an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
Order Form emplate"	the template in Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules);
Other Contracting uthority"	any actual or potential Buyer under the Framework Contract;
Outward xchange”	an exchange of Supplier Staff from the Supplier to the Buyer in accordance with the Secondment Agreement;
Overhead"	those amounts which are intended to recover a proportion of the Supplier’s or the Key Subcontractor’s (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
Parliament"	takes its natural meaning as interpreted by Law;
Party"	in the context of the Framework Contract, CCS or the Supplier, and in the context of a Call-Off Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits;
Performance ndicators" or Pls"	the performance measurements and targets in respect of the Supplier’s performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
Personal Data"	has the meaning given to it in the UK GDPR;
Personal Data reach”	has the meaning given to it in the UK GDPR;
Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Relevant Authority and/or their subcontractor and/or Subprocessor (as detailed in Joint Schedule 11 (Processing Data)) engaged in the performance of its obligations under a Contract;
Place of erformance”	the place or location at which the Deliverables, in whole or part, shall be performed;
Platform”	the platform, site or system (also known as ‘Contract-a-Thing’) operated on behalf of CCS which requires a potential Buyer to complete the Buyer Registration Procedure and specify its Authorised

	Users who may access and use the platform, site or system on behalf of the Buyer and use it to assist in selecting or shortlisting suppliers when undertaking a Call-Off Procedure in accordance with Framework Schedule 7, to Order Deliverables under a Contract;
Prescribed erson"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;
Pricing Matrix"	the pricing matrix of the Supplier may be found in the Platform and also in Annex 1 (Pricing Matrix) of Framework Schedule 3 (Framework Prices) which sets out the maximum Day Rates for each DDaT role for all Supplier Staff under the Contract;
Pricing echanism"	the pricing mechanisms are (a) Capped Time and Materials, (b) Incremental Fixed Prices, (c) Time and Materials, (d) Fixed Price, and (e) a combination of two or more of these as set out in Framework Schedule 3 (Framework Prices) and Framework Schedule 7 (Call-Off Award Procedure) and as may be refined in the Further Competition Procedure;
Pricing Tool"	the tool to be used by Buyers as part of the Call-Off Procedure which is set out in Annex D (Pricing Tool) of Framework Schedule 7 (Call-Off Award Procedure);
Processing"	has the meaning given to it in the UK GDPR;
Processor"	has the meaning given to it in the UK GDPR;
Progress eeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
Progress Meeting requency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
Progress Report requency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
Prohibited Acts"	a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for

	improper performance of a relevant function or activity in connection with each Contract; or c) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
Protective easures"	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
Recall"	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
Rectification lan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include: a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
Rectification Plan rocess"	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);
Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
Reimbursable xpenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance

	with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
Relevant uthority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
Relevant uthority's onfidential nformation"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and c) information derived from any of the above;
Relevant equirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
Relevant Tax uthority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
Reminder Notice"	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;
Replacement eliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
Replacement ubcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
Replacement upplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
Request For nformation"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;

Required nsurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
Resource"	the Buyer shall issue the Supplier and all Key Staff who are Off-Payroll Workers with a Status Determination Statement describing the IR35 status of each Supplier Staff in a key role or position being engaged to provide Services under the Contract;
Resource Profile"	the capacity of the Supplier to provide various DDaT roles aggregated at Role Family level and is designed to understand what skills are available from the Supplier and any named Subcontractors in terms of approximate number of Supplier Staff and the level of security clearance that must have been obtained by the Supplier Staff prior to commencement on a relevant Call-Off Contract;
Restricted Staff"	any person employed or engaged by either Party, in the capacity of director or in any research, technical, IT, security, engineering, procurement, financial, legal or managerial role who has been engaged in the provision of the Deliverables or management of the Contract either as principal, agent, employee, independent contractor or in any other form of employment or engagement over the previous 12 Months, directly worked with or had any material dealings, but shall not include any person employed or engaged in an administrative, clerical, manual or secretarial capacity;
Retained EU Law"	the category of UK Law created under Section 2 to 4 of the European Union (Withdrawal) Act 2018 at the end of the transition period following the repeal of the savings to the European Communities Act 1972;
Request for nformation" or RFI" Tool	the functional tool within the Platform (or as otherwise described in Framework Schedule 7 (Call-Off Award Procedure) to be used by Buyers to seek clarification or additional information from one or more suppliers that will assist the Buyer in preparing its Statement of Requirement, planning and conducting its Call-Off Procedure ,before undertaking a Call-Off Procedure in accordance with Framework Schedule 7 (Call-Off Award Procedure);
Role Family"	the grouping of related roles or professions which share common skills and capabilities;
Satisfaction ertificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
Scalability"	the potential size of the Supplier team needed to fulfil the Buyer requirements;
Secondment"	the temporary transfer of one or more Supplier Staff from the Supplier to the Buyer to another position or employment, in accordance with the Secondment Agreement for the Secondment Charge; and "**Secondee**" is a person on a Secondment;

Secondment greement"	the agreement entered into between the Supplier and Buyer regarding an Inward Exchange or an Outward Exchange or a Secondment which shall be in the form and format of the Call-Off Schedule 26 (Secondment Agreement Template);
Secondment harge"	the Charge for Supplier Staff on an Outward Secondment which shall be no more than the base salary and any relevant pension contributions ordinarily payable by the Supplier in respect of a Secondee (inclusive of VAT);
Security anagement Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
Self Audit ertificate"	the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
Serious Fraud ffice"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
Service apability"	the Service capabilities of the Supplier as set out in Annex 2 of Framework Schedule 1 (Specification) which are grouped under the following headings under which there are a number of sub-capabilities: 1. Performance analysis and data; 2. Security; 3. Service delivery; 4. Software development; 5. Support and operations; 6. Testing and auditing; 7. User experience; and 8. User research;
Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
Service Period"	has the meaning given to it in the Order Form;
Service rovision"	one or more of the service provisions set out in Paragraph 1.1 of Framework Schedule 1 (Specification);

Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form and each Statement of Work;
Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
Service Transfer ate"	the date of a Service Transfer;
Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
SME"	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 enterprises;
Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
Specific Change n Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form and, if applicable, each Statement of Work;
Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form, Statement of Work or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the

	date specified in the Order Form, and in the case of a Statement of Work, the date specified in that Statement of Work;
Statement of equirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
Statement of Vork" or "SOW"	the document which, upon execution by the Buyer and Supplier, shall become incorporated into their Call-Off Contract and it outlines the agreed body of works to be undertaken as part of the Call-Off Contract Deliverables. There may be any number of Statements of Work incorporated into a Call-Off Contract and each Statement of Work may include (but is not limited to) the Statement of Requirements, identified output(s), completion date(s) and charging method(s);
Status etermination tatement" or SDS"	a statement that describes the determination reached by the Buyer/client on the employment status (i.e. IR35 status) of an Off-Payroll Worker for a particular Call-Off Contract or any element of work undertaken as part of any SOW, and the reasons for reaching that determination. The SDS must be passed to the worker and the person or organisation the client contracts with for the worker's services;
SOW End Date"	the date up to and including this date when the supply of the Deliverables under the Statement of Work shall cease
SOW Start Date"	the date of the start of the Statement of Works as stated in the SOW;
Storage Media"	the part of any device that is capable of storing and retrieving data;
Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
Summary of Vork"	a short description of overview of the Buyer's Statement of Requirements;
Supplier"	the person, firm or company identified in the Framework Award Form;
Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
Supplier uthorised epresentative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;

Supplier ompliance fficer”	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
Supplier's onfidential nformation"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier’s attention or into the Supplier’s possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
Supplier quipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
Supplier arketing Contact"	shall be the person identified in the Framework Award Form;
Supplier Non-erformance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels; and/or c) comply with an obligation under a Contract;
Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
Supplier Profit argin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under a Contract;
Supporting ocumentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;

Tax”	a) all forms of taxation whether direct or indirect; b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
Termination otice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;
Test Issue"	any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract;
Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;
Tests "	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "**Tested**" and “**Testing**” shall be construed accordingly;
Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
Time and aterials”	a Pricing Mechanism whereby the Buyer agrees to pay the Supplier for the work performed by the Supplier Staff, based on no more than the pro rata division of the Day Rates by 7.5 to provide an Hourly Rate for the applicable grade of Supplier Staff who undertook the work (as set out in Annex 1 of Framework Schedule 3 (Framework Prices)) and for the materials used in the project based on pre-agreed material disclosures and subject to time approval by the Buyer;
Transferring upplier mployees"	those employees of the Supplier and/or the Supplier’s Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;

Transparency nformation"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and b) Commercially Sensitive Information;
Transparency eports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
UK GDPR"	the Retained EU Law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
User Terms"	the terms of use applicable to all Buyer's Authorised Users who access and use the Platform which are available at:[Insert link];
Variation"	any change to a Contract, including any change to a SOW under a Call-Off Contract;
Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
Variation rocedure"	the procedure set out in Clause 24 (Changing the contract);
VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
Worker ngagement tatus"	the details of the labour supply chain through which the Worker is engaged as Supplier Staff, for example, the Worker could be: (a) "employed by the Supplier the Buyer contracts with"; (b) "employed by another organisation within the supply chain, e.g. an agency or umbrella company"; (c) "an off-payroll worker engaged via an intermediary e.g. the worker's own personal service company"; or (d) "an independent sole trader";
Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;

Work Day"	a minimum of 7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the contract):

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** (**"CCS" / "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
[Statement of Work (SOW) reference:**]**	**[insert** SOW reference number and title (if applicable) or delete row]	
[Buyer reference:**]**	**[insert** cost centre/portfolio codes as appropriate**]**	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation	**[insert** detail here or use Annex 1 below]	
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: □ **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] □ **[reference Annex 1** as appropriate**]**	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]
[Timescale variation/s:**]**	**[insert** changes to dates/milestones or delete row]	

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature .....

Date .....

Name (in capitals) .....

Job Title .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in capitals) .....

Job Title .....

Address .....

.....

ANNEX 1

[insert details as required**]**

Joint Schedule 3 (Insurance Requirements)

1. The insurance the Supplier needs to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for the Contract Period and for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other

evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if the Supplier is not insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance to be provided

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Required amount of insurance

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from the Framework Start Date in accordance with this Schedule:

1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);

1.2 public liability and products insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and

1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality

Date: Details: Rates Duration of confidentiality: perpetual

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff to lodge deposits or identify papers with the employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world;

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world;

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 ensure all workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

5.1.3 ensure that use of overtime used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

1.3.1 this is allowed by national law;

1.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

appropriate safeguards are taken to protect the workers' health and safety; and

1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

1.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

2. Sustainability

2.1 The Supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled, unless the Buyer states to the contrary, to sub-contract its obligations under each Call-Off Contract to the Key Subcontractors set out in the Call-Off Order Form.

1.2 Subject to Paragraph 1.1, the Supplier is entitled to sub-contract some of its obligations under a Call-Off Contract to Key Subcontractors who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-Contract or replace a Key Subcontractor, it must obtain the prior written consent of the Buyer and the Supplier shall, at the time of requesting such consent, provide the Buyer with the information detailed in Paragraph 1.4. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. The Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the name and details of the directors, employees, agents, consultants and contractors of the subcontractor engaged in the performance of the Supplier's obligations under the Contract. Details should include: name; role; email address; address; contract details; Worker Engagement Route – for example, employed by subcontractor; engaged via worker's intermediary e.g. PSC (i.e. a personal service company), engaged as an independent sole trader or employed by another entity in supply chain;

1.4.3 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.4 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's length" terms;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

1.4.6 (where applicable) the Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by CCS and/or the Buyer, within 10 Working Days, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the buyer can end this contract) and 10.5 (When the supplier can end the contract) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to

the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Company; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; ii) non-payment by the Monitored Company of any financial indebtedness;

	iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company 3 in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier or any Key Subcontractor
"Rating Agencies"	6 the rating agencies listed in Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each

Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with sufficient working accounts to allow further validation of financial status to be undertaken.

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS and Buyers in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 [In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.]

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where CCS or Buyers reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 which CCS may share with Buyers) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

(a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

(b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.5 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it)

no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8 CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5;

5.1.3 in the case of the Buyer, the Supplier fails to agree a Financial Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) that ensures the continued performance of the Contract and delivery of the Deliverables under its Contract; and/or

5.1.4 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

ANNEX 1: RATING AGENCIES

Dun and Bradstreet ("D&B")

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default: Deadline for receiving the	[**Guidance:** Explain the Default, with clear Schedule, Clause and Paragraph references as appropriate] [**add** date (minimum 10 days from request)]		
[Revised] Rectification Plan:			
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default Anticipated impact	[**add** cause] [**add** impact]		
assessment:			
Actual effect of Default: Steps to be taken to	[**add** effect] **Steps**	**Timescale**	
rectification:	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete	[X] Working Days		
rectification of Default			
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review Reasons for rejection (if applicable)	[Plan Accepted] [Plan Rejected] [Revised Plan Requested] [**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(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.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an

applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational

measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: Redacted under FOIA Section 40 Personal Information
1.2 The contact details of the Supplier's Data Protection Officer are: **[Insert** Contact details]
1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: ● *As part of the delivery of their obligations under the Contract, the Supplier may be required to process and handle limited personal data as part of their contracted services including but not limited to:* ○ *if the Supplier is required to support the live service* ○ *during general user research as may be necessary* ○ *for development of new features* ○ *generating test data from real data* **The Supplier is Controller and the Relevant Authority is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph* 3 *to paragraph 16 of the following Personal Data:* ● *Not relevant for this contract* **The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:*

	● *Not relevant for this contract* **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* ● *Business contact details of Supplier Personnel for which the Supplier is the Controller,* ● *Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,*
Duration of the Processing	The duration of the Processing will be until the earliest of: • expiry/termination of the Contract • the date upon which the Processing is no longer necessary for the purposes of either party performing its obligations under the Contract (to the extent applicable)
Nature and purposes of the Processing	The nature of the processing could mean any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means). All personal data as described within this Schedule must be held and processed within the UK The purpose might include but not be limited to • user research • creation of test data • account creation and authentication • service management • feature development and user research • service incident investigation and user support • examination of logs
Type of Personal Data	The personal data could include: • full name and title • address, telephone number and email address • date of birth • gender • disability, health conditions and learning difficulties • driving licence number and entitlement details (provided by DVLA), disqualification dates and previous driving licence numbers

	• type of test - for an instructor theory test, we will also collect the personal reference number • the language requested for the test (English and Welsh) • information about past health and safety incidents that stop candidates from booking online • limited information about fraud and security incidents • payment details - including card holder's name, card holder's billing address, card number (numbers are encrypted and access is restricted), dates the card is valid from and to, issue number and card type (for example, MasterCard)
Categories of Data Subject	Data Subject as defined within Article 4 (1) of the GDPR Regulation (EU) 2016/679 could include: • Members of the public who are booking or taking DVSA Theory Tests • Trainers who are booking Theory Tests on behalf of candidates • Authority's personnel (including Contractors, Agency Workers and Temporary Workers) • Other Theory Test Delivery Partners and suppliers
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The data will be retained for the minimum time necessary for use by the Supplier and no longer than that as per the provided TTS Retention Schedule or where within the retention period, the Supplier must ensure that all data is returned to the Authority on termination of the contract and securely removed in compliance with the Security Requirements from any systems they have been using to deliver services under the contract.

Annex 2 - Joint Controller Agreement

Not used in this contract.

Joint Schedule 13 (Cyber Essentials Scheme)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Cyber Essentials Scheme"	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found at: https://www.cyberessentials.ncsc.gov.uk/
"Cyber Essentials Basic Certificate"	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
"Cyber Essentials Certificate"	Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate to be provided by the Supplier as set out in the Order Form
"Cyber Essential Scheme Data"	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
"Cyber Essentials Plus Certificate"	the certification awarded on the basis of external testing by an independent certification body of the Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. What Certification do you need

2.1 Where the Framework Award Form and/or Order Form requires that the Supplier provide a Cyber Essentials Plus Certificate prior to Framework Start Date and/or commencing the provision of Deliverables under the Call-Off Contract including, if applicable, any Statement of Work, the Supplier shall provide a valid Cyber Essentials Plus Certificate to CCS and/or the Buyer. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under the Call-Off Contract until such time as the Supplier has evidenced to CCS and/or the Buyer its compliance with this Paragraph 2.1.

2.2 Where the Supplier continues to process data during the Call-Off Contract Period the Supplier shall deliver to CCS and/or the Buyer evidence of renewal of the Cyber Essentials Plus Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.

2.3 In the event that the Supplier fails to comply with Paragraph 2.1 or 2.2, CCS and/or the Buyer reserves the right to terminate the Call-Off Contract for material Default.

2.4 The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Data contain provisions no less onerous on the Subcontractors

than those imposed on the Supplier under the Call-Off Contract in respect of the Cyber Essentials Plus Scheme under Paragraph 2.1 of this Schedule.

2.5 This Schedule shall survive termination or expiry of this Contract and each and any Call-Off Contract.

Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Project Performance	**Contract progress along with risks and issues**	Highlight report	Monthly
[Call-Off Contract Charges]	Charge Breakdown	**Excel spreadsheet**	Monthly
[Performance management]	Contract review report	Powerpoint	Monthly

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2. Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so

as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio

Call-Off Schedule 4 (Call Off Tender)

Redacted under FOIA Section 43, Commercial Interest

Crown Commercial Service

Call-Off Schedule 5 (Pricing Details and Expenses Policy)

1. Call-Off Contract Charges

1.1 The Supplier shall ensure:

1.1.1 as part of the Further Competition Procedure, its pricing for the Deliverables are in accordance with the Buyer's Statement of Requirements which shall be no greater than those based on the Framework Prices set out in Framework Schedule 3 (Framework Prices).

1.1.2 that all applicable Charges shall be calculated in accordance with the Pricing Mechanism detailed in the Order Form (and, if applicable, each SOW) using the following:

(a) the agreed Day Rates or other rates specified in this Schedule for Supplier Staff providing the Deliverables (which are exclusive of any applicable expenses and VAT);

(b) the number of Work Days, or pro rata portion of a Work Day, that Supplier Staff work solely to provide the Deliverables and meet the tasks sets out in the Order Form and, if applicable, each SOW (between the applicable SOW Start Date and SOW End Date).

1.2 Further to Paragraph 1.2 of Framework Schedule 3 (Framework Pricing), the Supplier will provide a detailed breakdown of its Charges for the Deliverables in sufficient detail to enable the Buyer to verify the accuracy of any invoice submitted.

This detailed breakdown will be incorporated into each SOW and include (but will not be limited to):

- a role description of each member of the Supplier Staff;
- a facilities description (if applicable);

- the agreed Day Rate for each Supplier Staff;
- any expenses charged for in relation to each Work Day for each Supplier Staff, which must be in accordance with the Buyer's Expenses Policy (if applicable);
- the number of Work Days, or pro rata for every part day, they will be actively be engaged in providing the Deliverables between the SOW Start Date and SOW End Date; and
- the total SOW cost for all Supplier Staff role and facilities in providing the Deliverables.

1.3 If a Capped Time and Materials or Fixed Price has been agreed for a particular SOW:

- the Supplier shall continue to work on the Deliverables until they are satisfactorily complete and accepted by the Buyer at its own cost and expense where the Capped or Fixed Price is exceeded; and
- the Buyer will have no obligation or liability to pay any additional Charges or cost of any part of the Deliverables yet to be completed and/or Delivered after the Capped or Fixed Price is exceeded by the Supplier.

1.4 All risks or contingencies will be included in the Charges. The Parties agree that the assumptions, representations, risks and contingencies detailed on each SOW will apply in relation to the Charges:

1.5 CPI (as defined by the Office of National Statistics) will be applied to all rates in year 3 and 4 of the contract.

The buyer will be invoiced monthly in arrears on a T&M basis unless an alternative cost model is agreed on any Statement of Work.

Annex 1 (Expenses Policy)

1. Travelling and subsistence expenses shall not exceed the upper limit of allowances payable to Departmental staff of equivalent status. Call-Off Schedule 5 (Call-Off Pricing) Crown Copyright 2021 Framework Ref: RM6263 Project Version: v1.0 Model Version: v3.1
2. Any travel undertaken as a consequence of performance of the Contract must utilise the most cost-effective means (taking into account the cost of travel, the

cost of meals and accommodation and savings in time) for the whole journey. Claims for travelling and subsistence must be related to the performance of duties for the purposes of this Contract and be certified as such. Visits abroad require the prior approval of the Department and should be pre-approved by SCS1 or above.

3. The current Departmental rates are shown below. These rates will apply for the duration of the Contract. Please see note below on rail travel. Travel by Motor Vehicles
4. **Motor mileage allowances for travel by private car and van:**

➢ Up to 10,000miles - 45 pence per mile (25p may apply if public transport is a viable alternative)

➢ Over 10,000 miles - 25 pence per mile Travel by Motorcycle 5. Motor mileage allowances for travel by private motorcycle and motorcycle combinations is 24 pence per mile.

Travel by Pedal Cycle. The pedal cycle allowance is 20 pence per mile.

Travel by Train . Travel by train should be by standard class (including Eurostar) - irrespective of grade, entitlement or distance - unless there are compelling reasons to travel first class or, exceptionally, a first-class discount ticket is cheaper. Any claim for travel other than standard class must be approved in advance by the Department.

Coach/Bus Travel Fares for official travel by coach, bus etc will be reimbursed.

Pricing template.

Redacted under FOIA Section 43, Commercial Interest

RM6263 DIGITAL SPECIALISTS AND PROGRAMMES - ATTACHMENT 4 PRICING SCHEDULE

Redacted under FOIA Section 43, Commercial Interest

Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Buyer Property"	**the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;**
"Buyer Software"	**any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;**
"Buyer System"	**the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;**
"Commercial off the shelf Software" or "COTS Software"	**Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms**
"Defect"	**any of the following:** a) **any error, damage or defect in the manufacturing of a Deliverable; or** b) **any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or**
	c) **any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or**

	d) **any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;**
"Emergency Maintenance"	**ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;**
"ICT Environment"	**the Buyer System and the Supplier System;**
"Licensed Software"	**all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;**
"Maintenance Schedule"	**has the meaning given to it in paragraph 8 of this Schedule;**
"Malicious Software"	**any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;**
"New Release"	**an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;**
"Open Source Software"	**computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;**

"Operating Environment"	**means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:** a) **the Deliverables are (or are to be) provided; or** b) **the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or** c) **where any part of the Supplier System is situated;**
"Permitted Maintenance"	**has the meaning given to it in paragraph 8.2 of this Schedule;**
"Quality Plans"	**has the meaning given to it in paragraph 6.1 of this Schedule;**
"Sites"	**has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;**
"Software"	**Specially Written Software COTS Software and non-COTS Supplier and third party Software;**
"Software Supporting Materials"	**has the meaning given to it in paragraph 9.1 of this Schedule;**
"Source Code"	**computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;**
"Specially Written Software"	**any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;**
"Supplier System"	**the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and**

	management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions on Intellectual Property Rights for the Digital Deliverables.

3. Buyer due diligence requirements

3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2. the actions needed to remedy each such unsuitable aspect; and

3.2.3. a timetable for and the costs of those actions.

3.3 The Supplier undertakes:

3.3.1 and represents to the Buyer that Deliverables will meet the Buyer's acceptance criteria as set out in the Call-Off Contract and, if applicable, each Statement of Work; and

3.3.2 to maintain all interface and interoperability between third party software or services, and Specially Written Software required for the performance or supply of the Deliverables.

4. Licensed software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the

Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels and Balanced Scorecard) and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

7.1. The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights

9.1. Assignments granted by the Supplier: Specially Written Software

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

a) of its own Existing IPR that is not COTS Software;

b) third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central

Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call-Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at Paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under Paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) Months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in Paragraph 9.2.

9.5. Licence granted by the Buyer

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to Paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. Malicious Software

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. IPR asset management

10.1 The Parties shall work together to ensure that there is appropriate IPR asset management under each Call-Off Contract, and:

10.1.1 where the Supplier is working on the Buyer's System, the Supplier shall comply with the Buyer's IPR asset management approach and procedures.

10.1.2 where the Supplier is working on the Supplier's System, the Buyer will ensure that it maintains its IPR asset management procedures in accordance with Good Industry Practice.

Records and materials associated with IPR asset management shall form part of the Deliverables, including those relating to any Specially Written Software or New IPR.

10.2 The Supplier shall comply with any instructions given by the Buyer as to where it shall store all work in progress Deliverables and finished Deliverables (including all Documentation and Source Code) during the term of the Call-Off Contract and at the stated intervals or frequency specified by the Buyer and upon termination of the Contract or any Statement of Work.

10.3 The Supplier shall ensure that all items it uploads into any repository contain sufficient detail, code annotations and instructions so that a third-party developer (with the relevant technical abilities within the applicable role) would be able to understand how the item was created and how it works together with other items in the repository within a reasonable timeframe.

10.4 The Supplier shall maintain a register of all Open Source Software it has used in the provision of the Deliverables as part of its IPR asset management obligations under this Contract.

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date and, if applicable, the Statement of Work will list the Key Roles and names of persons who the Supplier shall appoint to fill those Key Roles as of the SOW Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables;

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced;

1.5.6 on written request from the Buyer, provide a copy of the contract of employment or engagement (between the Supplier and Supplier Staff) for every member of the Supplier Staff made available to the Buyer under the Call-Off Contract when providing Deliverables, and under each Statement of Work;

1.5.7 on written request from the Buyer, provide details of start and end dates of engagement of all Key Staff filling Key Roles under the Call-Off Contract and, if applicable, under each Statement of Work[.[; and]

1.5.8 [**Insert** any additional requirements].]

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"BCDR Plan"	1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	3 the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
"Disaster Recovery Deliverables"	4 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	5 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	6 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	7 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	8 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	9 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

2.1 The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 At least ninety (90) Working Days after the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

2.2.2 the recovery of the Deliverables in the event of a Disaster

2.3 The BCDR Plan shall be divided into three sections:

2.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

2.3.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

2.3.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

6.1.1 on a regular basis and as a minimum once every six (6) Months;

6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree the Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year;

7.1.2 in the event of any major reconfiguration of the Deliverables

7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Call-Off Schedule 9 (Security)

Long Form Applies

Part A: Short Form Security Requirements

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	**the occurrence of:** a) **any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or** b) **the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,** **in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;**
"Security Management Plan"	**the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.**

2. Complying with security requirements and updates to them

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables, it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the

Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

6. Data security

6.1 The Supplier will ensure that any system on which the Supplier holds any Government Data will be accredited as specific to the Buyer and will comply with:

- the government security policy framework and information assurance policy (see: https://www.ncsc.gov.uk/collection/risk-management-collection);
- guidance on risk management (see: https://www.ncsc.gov.uk/collection/risk-management-collection);
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management and Accreditation of Information Systems (see: http://osgug.ucaiug.org/conformity/security/Shared%20Documents/Reference/UK%20-%20CPNI%20-%20Risk%20Management%20and%20Accreditation%20of%20IS.pdf); and
- the relevant government information assurance standard(s) (see: https://knowledgehub.group/documents/49300605/0/bps68723-0000-00-hmg-ia-standard-numbers-1-and-2-information-risk-management.pdf/645c3ec5-e187-8124-16e8-ab9d86540cbb?t=1605540161981).

6.2 Where the duration of a Call-Off Contract exceeds one (1) year, the Supplier will review the accreditation status at least once each year to assess whether material changes have occurred which could alter the original accreditation decision in relation to Government Data. If any changes have occurred then the Supplier agrees to promptly re-submit such system for re-accreditation.

Part B: Long Form Security Requirements

1. Definitions

1.1 In this Schedule the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

~~**"Baseline Security Requirements"**~~	~~**are the requirements set out in Part B, Annex 1 to this Schedule;**~~
"Breach of Security"	**means the occurrence of:** c) **any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or** d) **the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,** **in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d);**
"ISMS"	**the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and**
"Security Tests"	**tests to validate the ISMS and security of all relevant processes, systems, incident response**

	plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 Redacted under FOIA Section 40 Personal Information

2.3.2 [insert security representative of the Supplier]

2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the

ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of

the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d), the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures

which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d), any changes to the Security Policy; and

5.1.5 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d).

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

f) as soon as reasonably practicable, provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the

Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline Security Requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[ ]

Call-Off Schedule 10 (Exit Management)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Exclusive Assets"	Supplier Assets used exclusively by the Supplier [or a Key Subcontractor] in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Exit Plan"	the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier [or a Key Subcontractor] in connection with the Deliverables but which are also used by the Supplier [or Key Subcontractor] for other purposes;
"Registers"	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer

	receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for Contract exit and SOW exit

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables' IPR asset management system which includes all Document and Source Code repositories.

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Call-Off Contract Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of each SOW and this Contract.

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence whether this is in relation to one or more SOWs or the Call-Off Contract (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for

those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer a Call-Off Contract and SOW Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable (this may require modification to SOW Exit Plan provisions to be updated and incorporated as part of the SOW;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) prior to each SOW and no less than every [six (6) months] throughout the Contract Period; and

(b) no later than [twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [ten (10) Working Days] after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than [twenty (20) Working Days] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable, in the case of the Call-Off Contract and each SOW (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular

Service Levels or KPI, the Parties shall vary the relevant KPIs, Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-Contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 14B (Service Levels and Balanced Scorecard)

SECTION 1 SERVICE LEVELS

1. Definitions

1.1 In this Section 1 of this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Level Failure"	1 means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	2 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	3 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you do not meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.4.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.4.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure the Buyer shall be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"), provided that the operation of this Paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process; and/or

1.2.3 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Buyer redress for failure to provide Services at or above Service Levels

2.1 The Buyer may ask for a Rectification Plan if the Supplier fails to meet any number of the Service Levels in any 12-Month rolling period.

2.2 This Rectification Plan must clearly detail the improvements and associated timeframes within which the Supplier shall meet and achieve the Service Levels. The Rectification Plan must be provided in accordance with Clause 10.3 of the Core Terms and any failure to correct a Default in line with an accepted Rectification Plan, or failure to provide a Rectification Plan within 10 days of the request may result in

the Buyer exercising its right to terminate the Contract in accordance with Clause 10.4 of the Core Terms.

Annex A to Part A: Services Levels Table

Redacted under FOIA Section 43, Commercial Interest

Part B: Performance Monitoring

2. Performance Monitoring and Performance Review

2.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

2.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to Paragraph 1.1 of Part B of

Redacted under FOIA Section 43, Commercial Interest

this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

2.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

2.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

2.2.3 details of any Critical Service Level Failures;

2.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and

2.2.5 such other details as the Buyer may reasonably require from time to time.

2.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

2.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location, format and time (within normal business hours) as the Buyer shall reasonably require;

2.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

2.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

2.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

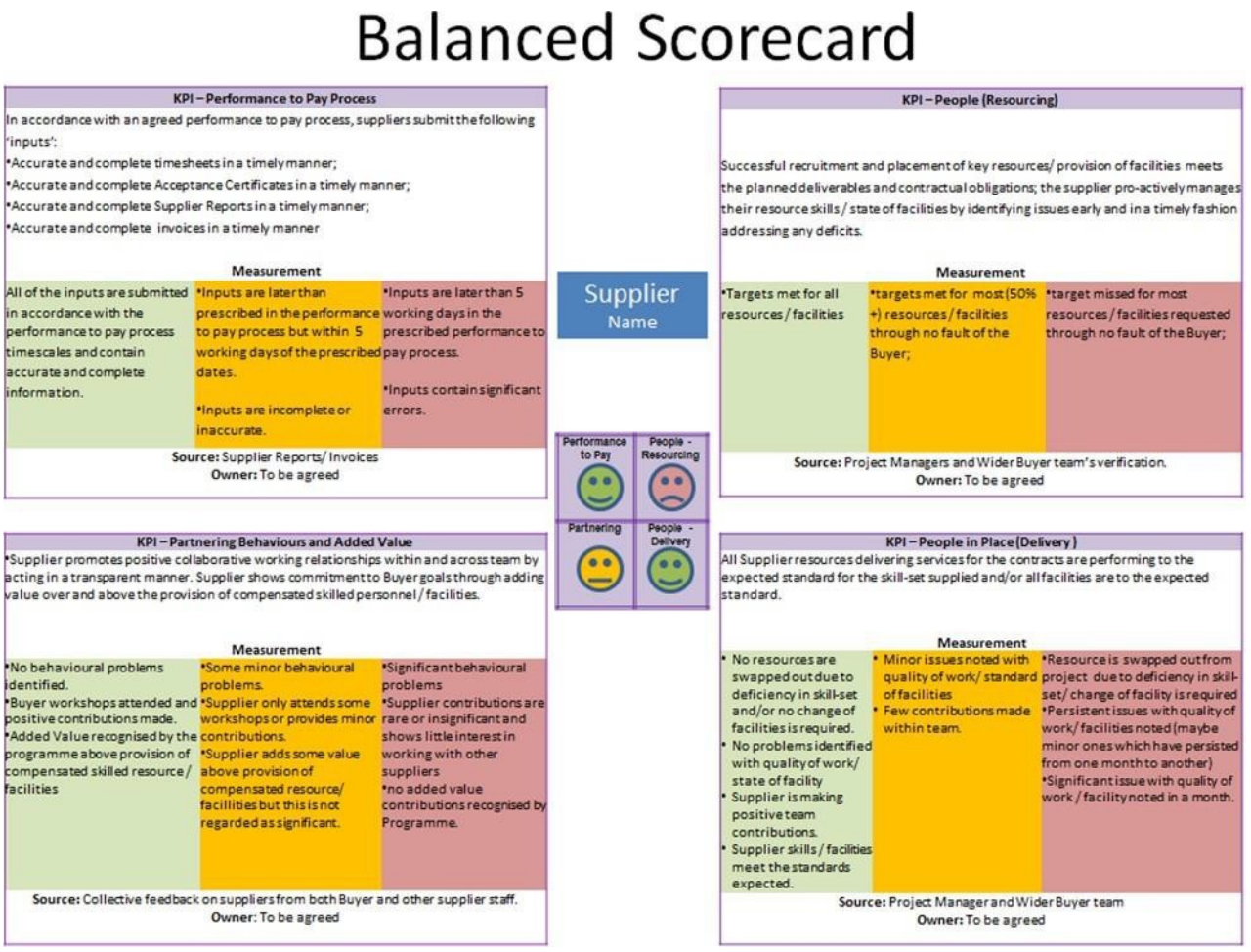
2.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier for any specified Service Period.

3. Satisfaction Surveys

3.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

SECTION 2 BALANCED SCORECARD

1.1 As an alternative to or in addition to Service Levels (under Section 1 above) and the Supplier's performance management obligations under the Framework Contract, the Buyer and Supplier may agree to follow the Balanced Scorecard and key performance indicators ("KPIs") for a Call-Off Contract and, if applicable, one or more of its Statements of Work.



1.2 The purpose of the Balanced Scorecard is to promote contract management activity through measurement of the Supplier's performance against KPIs. The Buyer and Supplier shall agree the content of the Scorecard before the Call-Off Contract Start Date including the Material KPIs as defined in Framework Schedule 4 (Framework Management). Targets and measures to be listed in the Scorecard (example above for guidance only) should be tailored to meet the Buyer's needs and the Supplier's competences.

1.3 The recommended process for using the Balanced Scorecard is as follows:

- the Buyer and Supplier agree a template Balanced Scorecard together with a performance management plan which clearly outlines the responsibilities and actions that will be taken if agreed performance levels are not achieved.

- on a pre-agreed schedule (for example, Monthly) both the Buyer and the Supplier provide a rating on the Supplier's performance

- following the initial rating, both Parties meet to review the scores and agree an overall final score for each KPI

- following agreement of final scores, the process is repeating as per the agreed schedule

2. Buyer redress for failure to provide Services at or above Service Levels

2.1 The Buyer may ask for a Rectification Plan if the Supplier:

2.1.1 fails to meet any of the Key Performance Indicators ("KPIs") listed within Annex A on at least [3] occasions within a 12-Month rolling period

2.1.2 demonstrates poor performance of a Call-Off Contract and, if applicable, any Statement of Work, evidenced through Buyer feedback to CCS that the Supplier has scored a 'red' status on any one of the [4] KPI targets listed in Annex A on at least [2] occasions within a Statement of Work duration, or within a period of 3Months (whichever is the earlier)

2.2 This Rectification Plan must clearly detail the improvements and associated timeframes within which the Supplier shall meet and achieve the KPI targets. The Rectification Plan must be provided in accordance with Clause 10.3 of the Core Terms and any failure to correct a Default in line with an accepted Rectification Plan, or failure to provide a Rectification Plan within 10 days of the request may result in the Buyer exercising its right to terminate the Contract in accordance with Clause 10.4 of the Core Terms.

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of KPIs in the Balanced Scorecard will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the

process and timescales agreed which shall contain, as a minimum, the following information in respect of the relevant KPIs just ended:

3.2.1 for each KPI, the actual performance achieved over the relevant period;

3.2.2 a summary of all failures to achieve KPIs that occurred during that period;

3.2.3 details of any failures of KPIs across the Call-Off Contract and, if applicable, each one or more SOW;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and

3.2.5 such other details as the Buyer may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location, format and time (within normal business hours) as the Buyer shall reasonably require;

3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier for any specified period.

Redacted under FOIA Section 43, Commercial Interest

Call-Off Schedule 15 (Call-Off Contract Management)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Managers in regards to the Contract and it will be the Supplier's Contract

Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call-Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Supplier Contract Review meeting to be held once per quarter remotely.

Call-Off Schedule 18 (Background Checks)

1. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

2. Definitions

"Relevant Conviction" means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

3.1.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

3.1.2 Notwithstanding Paragraph 3.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE);

(b) conduct thorough questioning regarding any Relevant Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

N/A

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

project

Specification

DVSA TTS Continuous Improvement and Legislative Change.

DVSA

Contract Reference: K280021880

CONTENTS

GLOSSARY In this Further Competition Invitation the following words and phrases have the following meanings:

*"**Authority**" means Driver and Vehicle Standards Agency;*

***"CCS"** means Crown Commercial Service;*

*"**Contract**" has the meaning set out in Framework Agreement Schedule 4;*

*"**Further Competition**" means the process used to establish a Contract that f f facilitates the provision of DVSA Continuous Improvement (Theory Test) Service*

*"**Further Competition** Template and **Invitation to Tender**" means this document and all related documents published by the Authority in relation to this Further Competition;*

***"In-House Theory Test Centres (IHTTC)"** means the organisations that the Authority has delegated authority to conduct theory tests for the employees "in-house" i.e. on their premises, using their equipment and staff.*

*"**Marking Scheme**" means the range of marks that may be given to a Potential Provider depending on the quality of its response to a question which is located in the boxes below the applicable question;*

*"**Minimum Total Score**" means the minimum score that the Potential Provider must obtain in order to be awarded the Contract;*

*"**Total Score Available**" means the maximum potential score that can be awarded for a response to a question;*

*"**Potential Provider**" means a company that submits a Tender in response to the Further Competition Invitation;*

*"**Supplier**" means the Potential Provider with whom the Authority has concluded the Contract;*

*"**Tender**" means the Potential Provider's formal offer in response to the Invitation to Tender;*

*"**Tender Clarifications Deadline**" means the time and date set out in paragraph 4 for the latest submission of clarification questions; and*

*"**Tender Submission Deadline**" means the time and date set out in paragraph 4 for the latest uploading of Tenders.*

***"Test Centre"** means a facility where tests are delivered in a secure invigilated space. The facility may be permanent or temporary and includes shared accommodation.*

***"Test Centre Network or TCN"** means the provider of Test Centre estate and facilities services to the Theory Test Service*

***"Test Engine and Test Content Management"** or **TETCM/TETCMS** means the technology capability that supports the test content lifecycle (create, update, delete), and the generation of the test form and test interface that is used by the Test Centre Networks and IHTTCs*

***"Trainer Booker"** means a driving instructor or trainer, who uses the service to book and manage driving and motorcycle tests on behalf of their pupils and who can name the candidate shortly before the test slot*

INTRODUCTION

The Authority is seeking the provision of a Continuous Improvement (Theory Test) Service for a period of 2 years with options to extend by a further 2 years (2+1+1). The very latest commencement date for this agreement will be 30th June 2023 although it is likely that services will commence sooner. The Authority will agree the commencement date with the successful supplier providing 4 weeks' notice for the supplier to mobilise the service

BACKGROUND TO THE REQUIREMENT

The Driver and Vehicle Standards Agency is an executive agency of the Department for Transport (DfT). On behalf of the Secretary of State for Transport (the "Authority"), one of the main functions of the Driver and Vehicle Standards Agency is to improve road safety in Great Britain by setting standards for driving and motorcycling, and for the education and training of drivers and riders. It is a requirement to pass a theory test as part of the process to gain driving licence entitlement for all vehicle categories. As part of the Authority's goal for improving road safety, it has responsibility for the strategy, policy and delivery of theory and practical driving and riding tests. This tender opportunity relates to the future of the Driver and Rider Theory Test Service ("TTS").

The TTS was introduced in 1996 and, until 2021, delivery was always outsourced as an end-to-end managed service to a single supplier. The current service uses a disaggregate supplier model – a test and content management supplier ("TETCM"), two suppliers of the nation test centre network ("TCN") and a central CRM / entitlement / booking / payment service.

There are two types of users of the TTS service; individual Candidates wishing to take a theory test and Business Users. There are two subsets of the Business Users category; Trainer Bookers who can book tests on behalf of individual Candidates and In-House Theory Test Centres ("IHTTC"), which are organisations to which the Authority has delegated authority to conduct theory tests for their employees "in-house" i.e. on their premises, using their equipment and staff. Content is presented to the Candidates and marked using the TTS test engine software. This software delivers the theory test into c.216 fixed estate and mobile testing facilities, which are the responsibility of the TCN providers. In addition, the IHTTC sites provide their own facilities but utilise the test engine software. Typically, over 2.5 million theory tests are conducted each year.

Under the current model, the Authority administers the test, in line with UK law, and maintains a layer of contract management and operational support.

The current model for delivering the theory test enables the Authority to:
Launch new revenue generating services which align to the theme of Lifetime of Safer Driving within the Authority strategy:
https://www.gov.uk/government/publications/dvsa-strategy-2017-to-2022

and support the Authority's road safety ambitions.
Improve the educational impact of learning and assessment services by more closely integrating the Authority's teams and arming them with fit for purpose tools, moving towards a 'learning journey' rather than a single point in time examination.
Proactively use data to analyse operational and test item performance, monitor service standards at a local level and provide evidence for policy making.
Design out inefficient activities and processes which exist in the current service.

A more flexible model to adapt to changes in technology and user preference:

- Advances in testing and education technology are creating new channels and methods of test delivery.

- Open source development and Agile methodologies are allowing digital services to be delivered at a lower lifetime cost, whilst constantly being improved to ensure services do not become outdated.
- Autonomous, connected and semi-autonomous vehicles will fundamentally change the nature of driving and therefore driving theory assessment will need to adapt to remain effective and relevant and therefore continue to deliver improved road safety outcomes.
- User preferences have also evolved, notably there is a trend towards self-service.
- The current service struggles to adapt quickly to exploit new opportunities and innovations and so the Authority wishes to adopt a more flexible model of delivery.

SCOPE

A high level view of the this requirement is:

Total contract value of up to £35m over 4 years which comprises the following key components:

1. Continuous Integration scope with a value of up to £8m over 2 years, plus 2 potential year extensions with a value of up to £4m per year.
2. Potential additional scope up to a value of £19m over 4 years which would cover additional improvements to the service.

Each identified work package would require business justification and be formally contracted though a separate statement of work against the total contract value.

The Authority is looking to confirm the supplier will have the capacity to address these additional improvement if required.

Delivery of software / process enhances to the central Theory Test CRM / entitlement / booking / payment service and integrations to other elements of the Theory Test

Deliver in agile manner using 2 week sprint cadence

Delivery of software packages with supporting user research, architecture, business analysis, software development and testing.

Responsibility for quality of deliverables, testing and production preparation of the delivered software

Work alongside Authority representatives to create pipeline of delivery

Collaboration with TSS to define any platform/environment requirements in a timely manner to enable successful delivery.

INTRODUCTION AND BACKGROUND TO THE AUTHORITY

Driver and Vehicle Standards Agency (DVSA) is an executive agency of the Department for Transport

We carry out driving tests, approve people to be driving instructors and MOT testers, carry out tests to make sure lorries and buses are safe to drive, carry out roadside checks on drivers and vehicles, and monitor vehicle recalls

We're responsible for:

- carrying out theory tests and driving tests for people who want to drive cars, motorcycles, lorries, buses and coaches, and specialist vehicles.
- approving people to be driving instructors and motorcycle trainers and making sure they provide good quality training.
- approving people to be MOT testers, approving the centres they work in, and testing lorries, buses and coaches ourselves.
- carrying out roadside checks on commercial drivers to make sure they follow safety rules and keep their vehicles safe to drive.
- monitoring recalls of vehicles, parts and accessories to make sure that manufacturers fix problems quickly.

- approving training courses for qualified drivers, such as Driver Certificate of Professional Competence courses for lorry, bus and coach drivers, and drink-drive rehabilitation courses
- supporting the Traffic Commissioners for Great Britain and the Northern Ireland transport regulator to license and monitor companies who operate lorries, buses and coaches, and to register local bus services.

BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

The Authority provides several digital services which are used by members of the public, MOT testers, licenced goods and passenger transport operators, and members of Authority staff involved in regulatory and administrative work.

These services support the Authority's core operations helping to meet its key objective of road safety. The scope of this contract is to provide CI and development for the Theory Test.

These teams are currently comprised of members of Authority staff, and team members from a contracted supplier. The team members work collaboratively to deliver outcomes defined within backlogs, owned, and prioritised by the Authority .

SPECIFICATION

The Authority is looking to procure the services of a digital services delivery partner, to deliver continuous improvement outcomes for one of the Authority's suite of digital services and products, in line with Government Central Digital & Data Office (CDDO), formerly GDS, service standards.

Our definition of Continuous Improvement (CI) is detailed within this document.

The Authority provides several digital services which are used by members of the public, MOT testers, licenced goods and passenger transport operators, and members of Authority staff involved in regulatory and administrative work. These services support the Authority's core operations helping to meet its key objective of road safety.

This document sets out the Authority's requirement for the over-arching service to be delivered. Each request for the supplier to deliver the service will be in a specific Statement of Work.

For guidance, there are typical scenarios in which the Authority would use this contract.

Deliver continuous improvement outcomes for the Theory Test digital services and products.
Build the Theory digital services to our standards and technical specification requirements.
To provide the service to enable the Authority to manage its priorities, for example to meet a legislative requirement.
The supplier will work collaboratively with the Authority's Digital Services Department. This will allow the Authority flexibility to maintain continuous improvement of its digital services.

CONTINUOUS IMPROVEMENT DEFINITION

The Authority has identified eight key outcomes of Continuous Improvement (CI) and this contract will procure a service to enable delivery of those outcomes:

Security

Data secure and in line with GDPR; compliance maintained with Cabinet Office and National Cyber Security Centre (NCSC); end-to-end security protections from current and emerging threats with >10,000 attempts per week. Just because a service is secure today

does not mean it will be secure tomorrow. A key outcome is ensuring that a service is able to maintain authority to operate. Additional security requirements detailed in Section 35.

Data

Ensure data is accurate and readily retrievable to support Authority needs and operations/enforcement.

Availability, Scalability and Stability:

Service is reliable, scaled to meet demand, with a remediation approach to issues – and to reduce risk of system failures.

Currency and Operability:

Software versions are up to date, with patching and maintenance – and to reduce risk of system failures.

Responsiveness, Adaptability, and Accessibility:

Service works on all modern devices and software, and in line with emergent regulations such as for accessibility and cookies.

Cost Optimisation of Cloud Platforms:

Architecture enhancements to stay aligned to Cloud developments – and to enable access to favourable commercial trading options for usage.

Developing the Service:

Meeting new policy, business and user needs to best meet policy objectives – and based on ongoing user research, feedback, and performance analysis.

Economies of Scale:

Working across Digital Services, the wider Agency and CDDO to identify opportunities for alignment, such as end-to-end user journeys, common architecture and design patterns, shared functionality and CDDO services such as payments.

Quality of Delivery:

All deliveries will encompass evidence based quality processes and use of embedded tools as a core part of the delivery. Quality processes will reviewed and updated as part of the continuous improvement

THE THEORY TEST SERVICE:

Target Operating Model

To achieve the Theory Test vision, the operating model has been designed around three broad components which, when combined, delivers the overall service to Business Customers and Candidates:

Service Operations – responsible for delivering the front-end testing services to the Business Customers and Candidates to continue delivering high standards and quality.

Service Development – responsible for the development and implementation of learning and test content, as well as continuously developing the quality of the TTS whilst ensure alignment and consistency of products.

Service Management – responsible for managing the overall delivery of the TTS using performance data and analytics.

High level architecture

The Theory Test service comprises the following services:

- Orchestration encompasses several distinct high-level components namely; integration layer, CRM, Data Repository, reporting interfaces and system logic components. Separate internal systems and third-party systems will need to interface with the platform through the integration layer, making the systems available to internal components.

- The CRM platform provides several workflow processes to facilitate the running of the service. Users for the workflows will include citizens, internal Authority staff and third-party suppliers.

- The Authority maintains integrity and ownership of the data across different parts of the service. The transactional data is persisted within the CRM system with the long-term (anonymised / aggregated) data and metric data being persisted within the Data Repository.

- Reporting and analytics are generated across the service to provide insights relating to KPIs and SLAs for all aspects of the TTS. This will include information provided by 3rd party suppliers which is aggregated to support the relevant reports.

- The table below provides a description of the containers and components identified in the target architecture in relation to the work the Potential Provider is required to carry out.

- the TTS overall IT system delivers an Authority function for orchestration, which IS responsible for:
  - Managing business processes/workflows through the CRM.
  - Managing the design and storage of data within the CRM.
  - Managing the integrations to other systems (internal to the Authority and external) through configuration of the integration layer.
  - Logic – includes process to 'move' data around the platform between for example; the CRM and Data Repository, the CRM and the TETCM.
  - Managing the Reporting and Analytic through dashboards and reports

Container Name	Responsibilities
TETCM (Test Engine / Test Content Management System)	The TETCM is responsible for: Providing a facility for the Authority to add and manage the test content Providing the Software to admit candidates into the Test Centres Providing the Software which runs on the workstations Providing Software to support Test Control, Test Generation, Invigilation, Test Feedback and Test Results
TCN (Test Centre Network)	The TCN is responsible for: Providing the slot availability within each provider's TCN to support the online booking process ("Scheduling") Access to Scheduling system interface

	Providing Test Centre Information 4. Providing staff and premises
Data Repository	The Data Repository is an export of MI data from the transactional system, which can then be used for other purposes, e.g. audit, reporting etc.
DVLA	DVLA integration is responsible for confirming candidate eligibility
Authority	The Authority's integration team is responsible for: Taking payments from the candidate / business (CPMS) Customer Payment Management System Finance and reconciliation (utilising SAP via shared service partner) Informing the Authority practical test booking system (TARS) Identity and access management ("Active Directory")
DVA	DVA integration is for Northern Ireland test takers and is responsible for: Candidate eligibility Storing results
Gov UK	Gov UK provide a number of Gov-Platform-As-A-Service (GPaaS) integrations, and will be responsible for: The static web content which will be used on the static pages of Gov UK for the theory test (Gov CMS) Notifying candidates by email/text (Notify) of their booking and/or reminder.
Other 3rd Party Services	Any other 3rd Party integrations that are currently known: Geo Location Search, which will be used as part of the booking process

The prioritised backlog is comprised of Stories (and bugs, spikes, tasks etc.) from different user perspectives across the different Continuous Improvement services.

Definitions can be found here https://www.gov.uk/service-manual/agile-delivery

INDIVIDUAL TECHNOLOGY STACKS

CRM

Dynamics CE (Customer Engagement) foundation extended and augmented as part of a more comprehensive Power Platform Solution (Power Apps, Power Automate, Dataverse). .

Candidate Booking Portal

Serverless web application built on Azure Functions (Typescript/node.js), Express, Nunjucks, HTML, SASS, Redis (sessions).

Trainer Booker Portal, IHTTC Portal, Incident Management Portal

3 different PowerApp Portals with the Dataverse from the Dynamics / CRM as the source. 2 of the Portals are government styled and assessed and the IM Portal is a customised version of the MS Case Management template.

Orchestration Tier

Serverless integration tier (REST APIs and SFTP/File transfer) built on Azure APIM, Functions (Typescript/node.js), OpenAPI/REST, Cosmos, Redis, Containers

Data Analytics & MI

Data pipelines and reporting DB built using Python, Synapse Link for Dataverse, Data Lake Storage, Azure SQL, DataBricks, Flyway, consumed by PowerBI.

CI DELIVERY OUTCOMES

CI delivery outcomes are defined in the product roadmap. A product Backlog will be defined, refined and prioritised in conjunction with the Authority. The delivery outcomes for each sprint will be jointly agreed and delivered to the expected quality with the agreed documentation

SERVICES THE SUPPLIER WILL PROVIDE TO DELIVER THE OUTCOMES

Supplier capabilities will include the following core skillsets

- Delivery Management
- Business Analysis
- Service Design
- Content Design
- User Research
- Architecture
- Software Development
- Quality Assurance and Test Management
- Performance Analysis
- Information Security
- Release Management

RESPONSIBILITIES

Authority responsibilities

The Authority will retain ownership and responsibility for maintaining its strategies and policies for:

- Architecture
- Technology
- Security
- Data Protection

The Authority will retain ownership of a number of corporate responsibilities. These are included in, but not limited to the list below, and may change during the course of the contract:

- Initiation of all work, governance, approvals, and funding processes.
- Strategy, and policies.
- All data within the systems worked on by the supplier.
- All Intellectual Property Rights.
- All data will be hosted on Authority systems in accordance with all appropriate security and data protection policies as directed by the Authority.
- The Authority will be responsible for oversight of all work carried out by the supplier.

A number of items will be worked on collaboratively between the Authority and supplier. The supplier will be responsible for providing expertise and solutions within the agreed frameworks, joint working and collaboration will be key to the success. Authority governance processes will

approve solutions and maintain overall ownership. These items are included in, but not limited to the list below, and may change during the course of the contract:

- All roadmaps for development.
- A prioritised backlog of work for the Theory Test digital service.
- All processes/ways of working.
- Objectives, delivery performance, specification of work.

BUSINESS REQUIREMENTS

To provide services for software development and delivery. Based on agreed roadmaps, sprint plans and defined outcomes

This work will deliver, security and stability, bug fixes and new enhancements ensuring technical currency of the existing digital services.

The supplier will deliver against the jointly agreed prioritised backlogs of work for the Theory Test service. The backlog will include CI backlogs; deliver new features based on user feedback, operability, technical currency or to support Policy change, and result in technically current services that are secure, maintainable, and extensible.

Where new features or updates to functionality are being introduced, training material may need to be provided to support a smooth implementation within the Authority. The requirements for training materials will be agreed between the Authority and Supplier as part of the product planning.

Collaboration

Supplier shall work collaboratively with and support the Authority and its other suppliers (e.g. TCN, TETCM, Technical Support Services, DVLA, DVA, Capita, CCDO) to ensure the successful delivery of all services related to the TTS. This applies to all elements of the TTS, from development, testing, integration, quality assurance and ensuring plans are coherent, transparent and exhaustive. Any stakeholder engagement requirements would be clear as part of the planning process. It will also include analysis and assistance on incidents where requested by the Authority or Technical Support Services.

The Supplier shall work collaboratively with the Authority to ensure suitable skills and knowledge transfer to the Authority's staff in order help to identify and build opportunities for in house capability where appropriate.

In order to ensure the effective delivery of the Authority's objectives, a number of required behaviours have been outlined. The Supplier will act in the following ways:

Collaborative Intention: the Supplier must act in good faith and adopt and maintain a genuine non-defensive presence and make a commitment to mutual success in its relationship with the Authority and the TTS Suppliers;

Openness: the Supplier must be honest in its dealings and open to honest feedback and create a culture of openness that allows all of the Supplier, the TTS Suppliers and the Authority to feel safe enough to discuss concerns, solve problems and deal directly with difficult issues;

Self Accountability: the Supplier must behave in a fair and reasonable manner and must take responsibility for its circumstances and the choices it makes either through its action or failing to act as well as the intended and unforeseen consequences of these actions. The Supplier must focus on the solution to a problem or issue rather than seeking to blame the Authority or any TTS Supp

Self-Awareness and Awareness of Others: the Supplier must commit to understanding its own organisations and issues within its own organisations as well as understanding concerns,

intentions and motivations of the Authority and the TTS Suppliers as well as the culture and context of the Authority and the TTS Suppliers' circumstances;

Problem Solving and Negotiating: the Supplier must proactively use problem-solving methods that promote a collaborative and co-operative atmosphere and avoid fostering covert, overt, conscious or unconscious enmity, conflicts or point-scoring;

Expertise: the Supplier shall commit to using its expertise to the benefit of the overall Theory Test Service and the end-to-end services delivered to the Authority and the Service Beneficiaries. The Supplier shall ensure that the Supplier Personnel work collaboratively with FTTS Supplier personnel, laying aside considerations of individual competitive advantage in the interests of the Authority;

Promote Value: the Supplier shall demonstrate a preparedness to innovate and adopt best practises and be forthcoming in initiating proposals for new best practices which deliver improved value to the Authority and the Service Beneficiaries;

Forward Looking: the Supplier shall take a forward looking approach that does not dwell on past issues or conflicts of delivery methods, other than ensuring that past lessons are learnt so as to maximise the effective delivery of end-to-end services to the Authority and the Service Beneficiaries;

Quality assurance requirements

This section deals with quality assurance requirements that the Supplier must deliver during the period of the Contract.

The Supplier will ensure that all quotations are accurate and reasonable for time and money.

The Supplier will utilise their expertise, skills and knowledge to make recommendations, where necessary, to the Authority. This will include any third party product recommendations

Following a Continuous Integration and delivery approach, it is intended that there will be incremental releases of functionality to a production (live) environment. The Authority will specify criteria for the acceptance of these releases and the Supplier staff will need to work with Authority and their support partners to ensure that these are met.

The Authority expects that the Supplier shall actively support each release of new functionality and will provide the immediate response to any critical and high severity defects identified within the agreed warranty period. Thereafter, responsibility will be passed to the Authority function and their support partners.

Quality of software delivery is essential for the Theory Test. The Supplier will warranty all software delivered into the production (live) environment for a period of 4 weeks after deployment to production. If a software bug / error is identified during this 4 week period, the Supplier will remediate at their own cost with no costs to the Authority.

Bugs/Errors identified by the Authority will have a root cause analysis undertaken by the supplier, which confirms both how the defect was introduced and how the bug was released through the quality process.

Acceptance criteria covering both functional and non-functional elements will be defined in advance for each item of work, which is aligned to an agreed 'Definition of Ready' and approved by DVSA Product Owners.

Analysis expertise will help define value and benefit for each piece of work in accordance with the agreed 'Definition of Ready'.

Items of work will be delivered to an agreed 'Definition of Done'.

Test evidence for sign-off is provided by the supplier in business oriented terms or technical assurance is provided by the supplier

Production of regular quality assessment reports will be provided, indicating how continuous improvements to quality processes can further improve. Additional actions for improvements will be centrally tracked and reported.

Performance of the contract will be managed by the Supplier delivery manager. They will work closely with the Authority service owner. There will be regular joint reviews against work in progress.

These reviews of progress will include, but not limited to:

- Tracking progress against roadmap plans and roadmaps
- Use of a timeboxed approach to delivery – to demonstrate completion to plan.
- Service management boards
- Review of risk/issues/decisions and dependencies (RAIDD) and escalation if necessary
- Emerging findings
- Costs incurred (running total)
- Review of upcoming work/next steps
- Review of resources
- Timescales for delivery – ensuring work is progressing to plan

The Authority follows the GDS Design Principles and Digital Service Standard to deliver public facing digital services, outlining the principles applied, methods adopted and ability to deliver successful outcomes.

CDDO Design Principles information can be found at:
https://www.gov.uk/guidance/government-design-principles

CDDO Service Standard information can be found at: https://www.gov.uk/service-manual/service-standard

TECHNICAL REQUIREMENTS

Suppliers will need to have experience in those technologies outlined below

Microsoft Dynamics 365 technologies – not limited to but includes

Microsoft Dynamics 365 technologies (including Dynamics for Customer Engagement), Microsoft Power Platform (including Dataverse, CDM, Apps, Automate, BI), C#, PowerApp Portals (Power Pages)

Microsoft Azure technologies – not limited to but includes

DNS Zone, Front Door, WAF, CDN, Vnets, Functions, Redis Cache, Service Bus, APIM, Key Vault, AppInsights, AAD (B2B and B2C), Containers, Cosmos, SQL, Storage – File/Blob/Data Lake, Synapse Link for Dataverse

General Infrastructure Tools and Infra as Code Tooling

Azure DevOps – pipelines, repositories, artifacts, GitHub, SonarQube, ARM templates, Powershell, Terraform, Docker, Incapsula Imperva, AlertLogic.

Production code:

C#, Typescript

Testing (Including automation):

Typescript/Jest, C#/xUnit, EasyRepro, JMeter, Postman, TestCafe/BrowserStack, SpecFlow/Selenium

AVAILABILITY

Services must remain highly available, secure, resilient, and technically current whilst built upon.

AUTHORITY TEAMS AND WAYS OF WORKING

Existing Authority Team

The Authority currently has these permanent roles within the Theory Test department:

Information Security analysts Service Owner Product Owner Technical Architect Reporting Analysts Business Analyst (Apprenticeship) Test Manager (Apprenticeship)	

Technical Support Services (TSS)

The Authority contracts a third party to provide technical support to the theory test taking total responsibility for the management of Theory Test services within the Azure production tenancy.

The scope of TSS is:

Maintenance, improvements and security of deployment pipelines and deployment release process for all Azure and CRM components and supporting infrastructure and environments (nonproduction and production environments)

Maturing relationship with Authority Cloud Infrastructure to implement Azure AD underpinnings for FTTS in line with overall Authority Azure Cloud Strategy

Progressing feature work infrastructure dependency changes in line with CI sprint timescales.

Accountable for the definition of deployment pipeline for all integrated environments (ops directory).

Development, maintenance, improvements and security of MI and Data Reporting Service

BUSINESS LOCATION

The Authority is working on a 'hybrid' model with staff working at a combination of office locations and from other suitable locations.

The Authority would accept a similar arrangement for supplier staff. Supplier staff may be required to work collaboratively with staff at Authority locations, with the remainder of the work being carried out remotely.

Remote working would be conducted using collaboration software that is available for Authority staff and any artefacts produced will be in formats that are usable by Authority staff.

The Authority mandates the use of the Atlassian (JIRA/Confluence) software for digital delivery

Key personnel will be required to attend in person for service management boards.

Supplier will demonstrate successful management of their staff working remotely.

The Authority key business location for this work is:

1 Unity Square, Nottingham NG2 1AW,
Travel to other locations may be required.

In order to provide analysis and assistance on incidents where requested by the Authority or Technical Support Services (clause 27.4), the Supplier must provide appropriately skilled staff who are located in the UK. These staff may be granted access to production data subject to appropriate security clearance to be agreed with DVSA.

BUSINESS CONTINUITY

In the event of a major business interruption affecting the supplier, we expect the Supplier to understand what their critical activities are in supporting the Authority, maintaining the capability to resume operations within agreed timeframes to ensure they provide an adequate service to the Authority. The Supplier will aim to minimise impacts using a focused, well managed response process and effective communications should a disruptive incident occur.

The Supplier will develop their own business continuity plan to support the overall Theory Test business continuity strategy.

In the event of a major business interruption the Supplier will deploy the required resources to implement their Business Continuity Plan. The Supplier will respond to the needs of the customer even if that means a potential reduction in normal service levels.

The Supplier will maintain a regular business continuity plan review process and will inform the Authority of any changes and/or improvements arising from this review.

The supplier will be required to take part in wider service business continuity testing and address actions from lessons learnt where required.

BUSINESS HOURS

The Authority's business hours are 0700 – 1900 Monday to Friday excluding Bank Holidays in England.

As part of this contract the Supplier staff will be expected to support out of working hours software releases where required.

SECURITY

Security Overview

The Supplier must consider security and privacy throughout the entire TTS Service solution lifecycle, including architecture and design, development, deployment and live operation processes where these are delivered under this Contract.

The Supplier shall ensure the TTS Service CI activities as delivered under this contract maintain the current level of security protection, which is audited to ISO 27001 and utilises a maturing suite of procedural and technical security controls

The Supplier (and subcontractors) shall meet the relevant clauses of the long form DSP Security Schedule during its fulfilment of the requirements of the Contract and the Security Management Plan must include but not be limited to the Delivery Partner's commitment t

Security Governance

Compliance with relevant legislation

Personnel security

Physical security of any supplier premises used to host DVSA data, code or artefacts

IT Security including where DVSA data, code or artefacts are held on the supplier'

Secure data transfer mechanisms

Incident management

Security testing

Audit requirements including audit by the DVSA as required

Security standards

The supplier (and any subcontractors used to deliver tasks under this Contract) must hold the following security certifications with the scope of certification fully covering the delivery of the services under this Contract:

a. ISO27001 from a UKAS certifying body

b. Cyber Essentials Plus

All work undertaken under the contract and solutions delivered must be compliant with/or aligns to the following industry and HMG standards:

a. AWS and Microsoft best security practice where relevant

b. NCSC Guidance and Principles

c. NIST security and cybersecurity standards

d. DVSA security policies (as provided)

e. DPA2018 and GDPR for handling personal data

f. General security good practice including but not limited to for example: management of secrets, management of vulnerabilities, auditing.

Security Governance

The Supplier shall contribute to the security governance of the TTS service by:

a. Attending the Orchestration monthly Security Working Group meetings plus other security meetings as requested by DVSA

b. Providing written/verbal contributions as requested by DVSA

c. Liaising with other internal DVSA system representatives, projects and third-party suppliers as requested by DVSA

d. Contribute to assessment of solution compliance with NIST standards

e. Providing a suitably qualified single security point of contact for DVSA who will attend meetings and provide liaison.

Security Artefacts

The Supplier must create or maintain suitable documentation to support the maintenance of a secure TTS solution and maintain DVSA Authority to Operate (ATO) such as (but not limited to):

a. Risk and impact assessments

b. Data Protection Impact Assessment and updates (where requested by DVSA)

c. Technical security architecture (s)

d. High Level Designs (HLDs)

e. Low level designs/configurations

f. Security Assurance Documentation

g. Change documentation

h. Release documentation

i. JIRA tickets relating to securit

j. Security testing scopes

k. Security testing reports

l. Security testing remediation plans

m. Security management processes/guidance

n. Security procedures

Artefacts must be kept up to date with agreed changes to the solution and services delivered under this Contract and must be reviewed for currency not less than quarterly.

Security risk management

The Supplier must ensure that the secure delivery of the services within this Contract continues to mitigate against the key risks to DVSA including (but not limited to):

a. *Loss of DVSA personal data*

b. *Loss/compromise of proprietary material*

c. *Unauthorised access to DVSA data*

d. *Non-repudiation of processing activity*

e. *Overall integrity of the DVSA Theory Test service and testing process*

f. *Availability of the existing DVSA Theory Test service and testing*

g. *Other connected DVSA and partner organisation services*

Data Protection

Delivery of this contract might require the supplier (or their subcontractors where specifically agreed with DVSA) to process Personal Data (as defined in the GDPR) on the DVSA's behalf.

The DVSA will be the Data Controller and the supplier will act as the Data Processor.

The supplier must process Personal Data only on the DVSA's documented instructions, as set out in DSP Schedule 11 (Schedule of Processing, Personal Data & Data Subjects) of the Contract and be subject to the full legal requirements placed upon them by GDPR.

Offshoring

The DVSA preference is for onshore arrangements to be in place.

DVSA may choose to consider proposals including offshoring whether inside the EEA or beyond Any proposal should include sufficient information to address the risks that DVSA would be looking to mitigate as part of such a solution. For example:

a. The country in which the data is to be processed needs to have a UK adequacy decision in place or where this is not the case, other control measures are in place such as standard contractual clauses.

b. Local laws and statutes may oblige organisations to provide access to DVSA data (including personal data and data relating to the security of DVSA systems) due to the

processing happening in that country. If it's an EU member state, we may be required to have a representative and a Data Protection Officer based within that country.

c. Additional mitigations for where there aren't equivalent standards e.g.

1. Physical security of the sites being used to house resource or data for the contract.

2. Vetting in the country of employment for resource.

Information about DVSA and access to DVSA systems are shared or accessed more widely that just the personnel working on the DVSA account.

Any changes to data being handled must be notified to, and agreed with, DVSA in advance. This includes the access of non-personal data from outside the U

If the proposal includes offshoring as part of the proposal, costs for DVSA to assure proposed arrangements should be included in the proposed costs. One visit to the proposed sites by 2 individuals should be include

Offshoring means:

a. the actual data being handled or processed outside the UK.

b. a backup copy of the data being handled or processed outside the UK.

c. IT support being able to access the data from outside the UK.

This also applies to any sub-contractors

Toolsets and environments

The Supplier must provide suitable controls and assurance of the tools used to deliver the contract including any development processes and environments such that:

a. Only assured tools as agreed with the DVSA are used to process DVSA data and artefacts

b. Access to any development and testing environments is controlled with auditable access controls lists, with formal auditable onboarding and offboarding processes and records

c. Devices allowed to access the development and testing environments must comply with NCSC guidance for End User Devices as a minimum standard.

d. Configuration control of development and testing environments is maintained and suitable monitoring of activity is carried out

***e.** Personal data is not used for testing or demonstration purposes unless suitably obfuscated and agreed with the DVSA*

Security Testing

The Supplier must arrange for an IT Health Check for the Supplier System in any of the following circumstances:

a. Prior to a grant of Authority to Proceed or Authority to Operate (e.g. events where the Supplier developed components or solutions are connected to the existing TTS services or external systems, loaded with Real Data or prior to live operation);

b. As part of the DVSA Security Assurance process integral to change management. Whenever any change is being planned for the existing TTS system that is assessed by the Change process as significantly impacting security, whether it relates to business processes,

software, infrastructure or ICT support processes. This includes significant releases in an Agile development.

c. Periodically, defined by risk, but generally at not more than 12-month intervals

The ITHC must be performed by a NCSC Green-light CHECK or CREST approved supplier

The Supplier must document and share with DVSA:

a. ITHC scopes

b. ITHC results

c. Identified vulnerabilities

d. Evidence for remediation

DVSA must be given the opportunity to approve any ITHC scopes in a timely manner prior to testing and attend daily feedback meetings as requested with the ITHC testing team

The Supplier shall ensure that ITHC observations are addressed by either:

a. Mitigating vulnerabilities in a timely manner as agreed with DVSA;

b. Obtaining formal acceptance of the vulnerability by DVSA

Security Audit

The Supplier must facilitate the DVSA to carry out security audits on its estate (and those of its subcontractors) where used to directly or indirectly deliver the services to the DVSA, including immediately without prior arrangement in response to a security alert or incident.

DVSA security audits will be agreed between the DVSA and the Supplier, and carefully planned to minimise disruptions to business processes.

Security training and awareness

The Supplier must ensure that its personnel go through regular mandatory data handling, data protection, cyber security awareness, and incident handling training to understand what an incident is, and how they should report it using the Supplier's incident handling processes. Training must inform users of good security practices, such as locking their computer, not using untrusted USB devices etc

Security Incident Management

The Supplier must have an incident handling approach that is able to align with the DVSA's extant processes. The Supplier must ensure that any necessary people, data and systems are made available to the DVSA to support the handling, resolution and investigation of an incident.

An incident is any event or action that breaches information security policies and procedures or which compromises, or threatens to compromise, the confidentiality, integrity or availability of

information, assets, the communications infrastructure or IT equipment that is being used by the Supplier and their contractors to deliver the services under this contract to DVSA.

Incidents include, but aren't limited to:

a. breaches of physical security.

b. detection or introduction of malicious code.

c. inappropriate content.

d. inappropriate or unauthorised access of IT services or information.

e. malfunctions of software.

f. misuse of information, items and/or equipment.

g. theft or loss of information, items and/or equipment.

h. unauthorised destruction of information.

i. unauthorised disclosure of information.

j. uncontrolled system changes.

k. unsecure information, items and/or equipment.

l. violations of network and system access.

The Supplier must inform the DVSA as soon as possible of observing an incident (including weekends and weekdays, public holidays).

The Supplier must assist the DVSA in determining and implementing measures and processes to handle an incident. The DVSA will assess incidents and determine if they are to be classified as near misses, security weaknesses or incidents and what actions, if any, are to be taken to mitigate them.

Security Clearance

For all individuals (including subcontractors) a Baseline Personnel Security Standard (BPSS) must be undertaken for their staff before they begin working on this contract.

Details of which can be found here:

https://www.gov.uk/government/publications/unitedkingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels.

For any individuals offshore a BPSS equivalent must be agreed with DVSA and undertaken.

DVSA and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable DVSA to determine which roles require additional vetting such as a specific National Security vetting clearance (e.g. a Counter Terrorist Check; a Security Check).

Roles which are likely to require additional vetting include system administrators, security team members, developers and system architects whose role would provide those individuals with

privileged access to IT systems which process large volumes of personal data, security data or data which is classified as OFFICIAL-SENSITIV

Any individuals requiring additional clearances as agreed with DVSA must have completed the vetting process prior to access being granted

Data Deletion

During the contract the supplier and any relevant subcontractors must:

a. securely erase any or all DVSA Data held by the Supplier when requested to do so by the DVSA; and

b. securely destroy all media that has held DVSA Data at the end of life of that media in accordance with any specific requirements in the Contract and, in the absence of any such requirements, as directed by the DVSA

c. securely destroy DVSA Data only on sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001; and

d. are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the DVSA

.

SOCIAL VALUE

In September 2020, the Government implemented measures to promote new jobs and skills, encourage economic growth and prosperity, tackle climate change and level up the UK. Social value is included in the procurement model and will be used by government departments to assess a supplier's social impact.

This approach will mean more opportunities for SMEs and social enterprises to win Government contracts by demonstrating the full extent of the value they would generate.

Value for money will still be paramount, but a bidder's social value score will be incorporated into assessment of contracts.

Government departments will use the social value model to assess and score suppliers on the wider positive benefits they bring by delivering the contract. This will mean that value for

money for the taxpayer can be maximised while also building a more resilient and diverse supplier base

The social value model which departments will assess contracts on includes:

Supporting COVID-19 recovery, including helping local communities manage and recover from the impact of COVID;

Tackling economic inequality, including creating new businesses, jobs and skills, as well as increasing supply chain resilience;

Fighting climate change and reducing waste;

Driving equal opportunity, including reducing the disability employment gap and tackling workforce inequality Improving health and wellbeing and community integration.

This approach will apply tests that all bidders, irrespective of their size and type, will be capable of meeting and therefore further levels the playing field for the UK's small businesses, start-ups and voluntary and community sector organisations and social enterprises.

The Authority will be assessing evidence of how suppliers are driving equal opportunity by tackling workforce inequality.

All Potential Providers are required to include within their response to tender evidence of how they create opportunities to tackle training, employment, skills and pay inequality in the contract workforce, or to support in-work progression to help people in the contract workforce to move into higher paid work by developing new skills relevant to the contract.

***To note:** It is a legal requirement for companies with 250 employees or more to publish their annual gender pay data on-line*

The Authority has selected this criterion as relevant to underpinning the delivery of services within the contract, and as being aligned to its own equal opportunities and inclusion policies.

More information about the Social Value Model used for government procurement is at:
https://www.gov.uk/government/news/new-measures-to-deliver-value-to-society-through-public-procurement

SKILLS AND EXPERIENCE

Essential Skills and Experience

The Authority will use the listed skills and experience to help them evaluate suppliers' technical competence.

Software Developmen

Experience of full software development lifecycle

Experience of REST API design.

Expertise with developer best practice including pair programming, code reviews, TDD.

Experience of developing in Microsoft Azure cloud-based digital services at scale.

Experience with Runtimes and Languages: C#, Typescript, Node.js.

Experience with web frameworks – particularly Node Express

Experience of Microsoft Dynamics and Power Platform technologies, including customisation/plugins/extensions, use of low-code solutions, and automation of testing and deployment to enable continuous integration

Experience of Version control systems: Git, (Azure DevOps, Github)

Knowledge of distributed systems

Knowledge of relational database technologies (e.g., Azure SQL).

Knowledge of No-SQL storage systems (e.g., Cosmos DB)

Awareness of public sector work e.g., UK Government CDDO.

Experience working with Azure managed Services, Front Door, WAF, CDN, VNets, Functions, Redis Cache, Service Bus, APIM, Key Vault, AppInsights, AAD (B2B and B2C), Containers, Storage – File/Blob/Data Lake.

Experience with general Infrastructure tools and Infra as code tooling: Azure DevOps pipelines, ARM templates.

Awareness of NCSC cloud security principles for service security.

Experience of OWASP Application Security Verification Standard for application development and testing.

Awareness of static analysis tools and code quality tooling

Awareness of Semantic and Accessibility Web Standards (W3C, WCAG)

Software Testing

Experience with Automated testing and test engineering in an Agile environment

Experience in forming and following test plans and strategies

Experience of non-functional testing and tooling

Experience of API and Microservices Architecture testin

Experience of Performance and load testing, and creating representative performance test scenarios from measured production end user behaviour

Experience of Typescript, Jest, TestCafe, BrowserStack, Postman, and other automated testing tools

Experience with automating the regression testing of Microsoft Dynamics/Power Platform and low-code solutions

Experience with JMeter and other performance testing tools

Experience with Docker

Experience of Version control systems: Git, (Azure DevOps, Github)

Experience of CI / CD tooling: Azure DevOps pipelines

Architecture

Significant and proven experience of architecting highly available, fault tolerant solutions on Microsoft Azure.

Deep understanding and experience of various software architectures (Serverless and Microservices) and methodologies

Deep understanding and experience of various Microsoft Dynamics and Power Platform technologies, including customisation/plugins/extensions, use of low-code solutions, and automation of testing and deployment to enable continuous integration

Fluent in architectural design techniques with experience of facilitating development of architectural plans.

Great at documenting your solutions in a way that varied audience can understand.

Experience of emergent architecture and shared services patterns.

Experience with managing technical debt

Data

Relational database services (both relational and non-relational or NoSQL) within cloud providers

Experience with Data Lake architectures and real-time data pipelines hosted in Microsoft Azure

Experience with cloud-based recovery strategies

Experience with both support and design

Experience and understanding of database design and how this is impacted by usage

Experience of monitoring strategies within a cloud environment

Experience with DB performance tuning, query optimisation and troubleshoot

Experience and knowledge of mitigation strategies during change

Delivery Management

Skills and experience in delivery roles consistent with the technologies (listed above) to deliver large scale cloud-based digital services.

Experience of agile delivery.

Version control.

Experience with developing CI/CD delivery pipelines.

Experience with managing technical debt

Experience in documenting technical solutions so that they are understood by a wide range of readers (e.g., non-technical staff).

Service Design

Experienced with Service Design including problem framing, customer journey mapping, service blueprinting, end to end service mapping, and facilitation of multiple stakeholders in meetings and workshops.

Experienced with user research strategy and execution to demonstrate user needs-based development.

Experience of customer journey performance analysis and evaluation demonstrating understanding of user behaviour and highlighting future improvement opportunities.

Experienced with business analysis including problem framing, business process modelling and improvement, value/benefits definition, scope definition, user story definition and management, stakeholder management and facilitation, success criteria definitio

Accessibility

The Authority is committed to delivering public services that are accessible to all. This includes complying with the Public Sector Bodies Accessibility Regulations (PSBAR) 2018 by ensuring our services meet the Web Content Accessibility Guidelines (WCAG) 2.1. All services must meet this standard to a minimum of AA level or have a clear and timebound road map towards meeting the standard. This commitment is embodied in the accessibility statements that each service publishes. Compliance with the regulations and the standard is monitored and enforced by the CDDO.

Experience of using these standards to deliver public facing digital services.

CDDO Design Principles

Experience of using CDDO Design Principles and Digital Service Standard to deliver public facing digital services, outlining the principles applied, methods adopted and ability to deliver successful outcomes.

CDDO Design Principles information can be found at:

https://www.gov.uk/guidance/government-design-principles

CDDO Service Standard information can be found at:

https://www.gov.uk/service-manual/service-standard

Content Design

Experience of using CDDO content design standards. Information about CDDO content design standards is at:

https://www.gov.uk/guidance/content-design

Knowledge Transfer

Experience of good practices around documentation/knowledge transfer as standard ways of working. Examples Include:

- Business process diagrams
- Technical information
- Annotated code
- User research outputs
- Customer journey maps
- Service blueprints
- Prototypes

Experience with CDDO audit and assessment

Experience coaching partners and teams with Agile practice

IMS

Experience in understanding and defining system security requirements.

Experience of preparing and documenting standard operating procedures and protocols.

Configure and troubleshoot security infrastructure devices.

Develop technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.

Facilitate in the detection and remediation of security incident

Write comprehensive reports, including assessment-based findings, outcomes and propositions for further system security enhancement.

All staff must be entitled to the appropriate security clearance as outlined in Section 35.19

Data Protection

Experience of ensuring staff involved in data processing receive appropriate guidance and training.

Experience of conducting compliance audits as required to ensure compliance and address potential issues proactively.

Experience of serving as the point of contact between CI teams and IMS Data Team

Experience of monitoring compliance and provide advice on the impact of new uses of data within projects/services and involving third parties.

Further Requirements

The supplier must be able to demonstrate a culture of continuous improvement.

PERFORMANCE MANAGEMENT

Performance for the contract will be managed by regular reviews against work in progress as specified in Statements of Work (SoW). Reviews of progress will include

- *Tracking progress against roadmaps*
- *Use of a timeboxed approach to delivery – to demonstrate completion to plan.*
- *User story mapping*
- *Epics/sizing*
- *Sprint reviews – reporting/backlogs/burndown charts (to show completion, velocity, continuous improvement of team performance) with specific attention on variance what was planned versus what was delivered.*
- *Service management boards*
- *Services for the candidate portal are delivered in line with CDDO and Authority standards (coding standards for example). Trainer Booker portal, IHTTC portal, incident management portal are not public facing.*
- *Analysis of first month critical bugs identified in production against the SoW.*

Work to be delivered by the supplier as part of this contract will be specified in a specific SoW to be agreed between the Authority and the Supplier.

Each SoW will include:

Specific measurable deliverables, including metrics;

Timescales for delivery

Supplier cost of delivery

Worker Engagement Status (including IR35 status)

Core CI service delivery is deemed in scope of IR35. Any specific delivery requirements as a result of changes to legislation will be assessed individually and the IR35 status confirmed on each Statement of Work.

Driver & Vehicle Standards Agency

Further Competition

For

DVSA TTS CI and Legislative Change

Contract: K280021880

Under Framework RM6263 Digital Specialists and Programmes

Helping you **stay safe** on **Britain's roads**

Document Reference	Further competition document	**Version No.**	V2.0
Author	Redacted under FOIA Section 40, Personal Information	**Date**	9 December 2022
Owner	Redacted under FOIA Section 40, Personal Information	**Status**	Final
Issued date		**Review date**	
December 2022		Fixed – None Planned	

Version control

Date	Version	Status	Changes
30/11/2022	1.1		Changes made to tender timeline table
2/12/2022	1.2		Addition of Q8 and amendments to guidance on costs
9/12/2022	2.0		Change to cost/quality weightings

1 Glossary

1.1 In this Further Competition Invitation the following words and phrases have the following meanings:

1.2 “Buyer” means [Driver & Vehicle Standards Agency (DVSA);

1.3 “CCS” means Crown Commercial Service;

1.4 “Further Competition” means the process used to establish a Contract that facilitates the provision of DVSA TTS CI and Legislative Change;

1.5 “Further Competition Template and Invitation to Tender” means this document and all related documents published by the Buyer in relation to this Further Competition;

1.6 “Marking Scheme” means the range of marks that may be given to a Potential Provider depending on the quality of its response to a question which is located in the boxes below the applicable question;

1.7 “Minimum Total Score” means the minimum score that the Potential Provider must obtain in order to be awarded the Contract;

1.8 “Total Score Available” means the maximum potential score that can be awarded for a response to a question;

1.9 “Potential Provider” means a company that submits a Tender in response to the Further Competition Invitation;

1.10 “Supplier” means the Potential Provider with whom the Buyer has concluded the Contract;

1.11 “Tender” means the Potential Provider’s formal offer in response to the Invitation to Tender;

1.12 “Tender Clarifications Deadline” means the time and date set out in paragraph 4 for the latest submission of clarification questions; and

1.13 “Tender Submission Deadline” means the time and date set out in paragraph 4 for the latest uploading of Tenders.

1.14 “Authority” means Driver and Vehicle Standards Agency

1.15 “In-House Theory Test Centres (IHTTC)” means the organisations that the Authority has delegated authority to conduct theory tests for the employees “in-house” i.e. on their premises, using their equipment and staff.

1.16 “Test Centre” means a facility where tests are delivered in a secure invigilated space. The facility may be permanent or temporary and includes shared accommodation

1.17 “Test Centre Network or TCN” means the provider of Test Centre estate and facilities services to the Theory Test Service

1.18 “Test Engine and Test Content Management” or TETCM/TETCMS means the technology capability that supports the test content lifecycle (create, update, delete), and the generation of the test form and test interface that is used by the Test Centre Networks and IHTTCs

1.19 “Trainer Booker” means a driving instructor or trainer, who uses the service to book and manage driving and motorcycle tests on behalf of their pupils and who can name the candidate shortly before the test slot

2 Introduction

2.1 This Further Competition Invitation relates to the Further Competition to award a DVSA TTS CI and Legislative Change Contract to a sole Supplier.

2.2 This Further Competition Invitation contains the information and instructions the Potential Provider needs to submit a Tender.

2.3 This Further Competition is being conducted under the CCS Digital Specialists & Programmes Framework – RM6263.

2.4 The Authority is seeking the provision of a Continuous Improvement (Theory Test) Service and delivery of Legislative changes for a period of 2 years with options to extend by a further 2 years (2+1+1). The very latest commencement date for this agreement will be June 2023 although it is likely that services will commence sooner. The Authority will agree the commencement date with the successful supplier providing 4 weeks’ notice for the supplier to mobilise the service.

3 Background to the Requirement

3.1 The Driver and Vehicle Standards Agency is an executive agency of the Department for Transport (DfT). On behalf of the Secretary of State for Transport (the “Authority”), one of the main functions of the Driver and Vehicle Standards Agency is to improve road safety in Great Britain by setting standards for driving and motorcycling, and for the education and training of drivers and riders. It is a requirement to pass a theory test as part of the process to gain driving licence entitlement for all vehicle categories. As part of the Authority’s goal for improving road safety, it has responsibility for the strategy, policy and delivery of theory and practical driving and riding tests. This tender opportunity relates to the future of the Driver and Rider Theory Test Service (“TTS”).

3.2 The TTS was introduced in 1996 and, until 2021, delivery was always outsourced as an end-to-end managed service to a single supplier. The current service uses a disaggregate supplier model – a test and content management supplier (“TETCM”), two suppliers of the nation test centre network (“TCN”) and a central CRM / entitlement / booking / payment service.

3.3 There are two types of users of the TTS service; individual Candidates wishing to take a theory test and Business Users. There are two subsets of the Business Users category; Trainer Bookers who can book tests on behalf of individual Candidates and In-House Theory Test Centres (“IHTTC”), which are organisations to which the Authority has delegated authority to conduct theory tests for their employees “in-house” i.e. on their premises, using their equipment and staff. Content is presented to the Candidates and marked using the TTS test engine software. This software delivers the theory test into c.216 fixed estate and mobile

testing facilities, which are the responsibility of the TCN providers. In addition, the IHTTC sites provide their own facilities but utilise the test engine software. Typically, over 2.5 million theory tests are conducted each year.

3.4 Under the current model, the Authority administers the test, in line with UK law, and maintains a layer of contract management and operational support.

3.5 The current model for delivering the theory test enables the Authority to:

- Launch new revenue generating services which align to the theme of Life-time of Safer Driving within the Authority strategy:
- https://www.gov.uk/government/publications/dvsa-strategy-2017-to-2022, and support the Authority's road safety ambitions
- Improve the educational impact of learning and assessment services by more closely integrating the Authority's teams and arming them with fit for purpose tools, moving towards a 'learning journey' rather than a single point in time examination.
- Proactively use data to analyse operational and test item performance, monitor service standards at a local level and provide evidence for policy making.
- Design out inefficient activities and processes which exist in the current service.

3.6 A more flexible model to adapt to changes in technology and user preference:

- Advances in testing and education technology are creating new channels and methods of test delivery.
- Open source development and Agile methodologies are allowing digital services to be delivered at a lower lifetime cost, whilst constantly being improved to ensure services do not become outdated.
- Autonomous, connected and semi-autonomous vehicles will fundamentally change the nature of driving and therefore driving theory assessment will need to adapt to remain effective and relevant and therefore continue to deliver improved road safety outcomes.
- User preferences have also evolved, notably there is a trend towards self-service.
- The current service struggles to adapt quickly to exploit new opportunities and innovations and so the Authority wishes to adopt a more flexible model of delivery.

4 Scope

4.1 A high level view of the this requirement is:

4.1.1 Total contract value of up to £35m over 4 years which comprises the following key components:

Continuous Integration scope with a value of up to £8m over 2 years, plus 2 potential year extensions with a value of up to £4m per year.

Potential additional scope up to a value of £19m over 4 years which would cover additional improvements to the service.
Each identified work package would require business justification and be formally contracted though a separate statement of work against the total contract value.
The Authority is looking to confirm the supplier will have the capacity to address these additional improvements if required.

4.1.2 Delivery of software / process enhances to the central Theory Test CRM / entitlement / booking / payment service and integrations to other elements of the Theory Test

4.1.3 Deliver in agile manner using 2 week sprint cadence

4.1.4 Delivery of software packages with supporting user research, architecture, business analysis, software development and testing.

4.1.5 Responsibility for quality of deliverables, testing and production preparation of the delivered software

4.1.6 Work alongside Authority representatives to create pipeline of delivery

4.1.7 Collaboration with TSS to define any platform/environment requirements in a timely manner to enable successful delivery.

5 Overview of Invitation to Tender

5.1 The following appendices accompany this ITT:

5.2 Appendix A – Terms of the Further Competition

Sets out rights and obligations which apply to the Potential Provider and the Buyer during this Further Competition as per the core clauses of the contract, alternative and additional provisions and specific standards.

5.3 Appendix B – Specification services under the relevant Lot

A detailed description of the Services that the Supplier will be required to supply to the Buyer.

5.4 Appendix C – Further Competition Questionnaire

The questionnaire created by the Buyer, is used to test the suitability of the Potential Providers to meet necessary criteria in order to provide the required services. This is used to provide final scoring and decide the successful supplier. **Please note that Appendix C is for information only and that all answers must be entered into the Jaggaer e-sourcing system.**

6 Further Competition Timetable

6.1 The timetable for this Further Competition is set out in the table below.

6.2 The Buyer may change this timetable at any time. Potential Providers will be informed if changes to this timetable are necessary.

6.3 The Buyer must receive all Tenders before the Tender Submission Deadline.

6.4 Tenders after the Tender Submission Deadline may be rejected by the Buyer to ensure that all Potential Providers are treated fairly. The decision whether to reject a Tender received after the Tender Submission Deadline is made entirely at the Buyer's discretion.

Date	Activity
5th December 2022	Publication of the Further Competition Invitation
5th December 2022	Clarification period starts
13th December 2022	Clarification period closes ("Tender Clarification Deadline")
15th December 2022	Deadline for the publication of responses to Tender Clarification questions
22nd December 2022	Deadline for submission of a Tender to the Buyer Contract ("Tender Submission Deadline")
January 2023	Evaluation
20th February 2023	Start date of 10-day Standstill period
April 2023	Expected commencement date for the Contract

7 Questions and Clarifications

7.1 Potential Providers may raise questions or seek clarification regarding any aspect of this Further Competition at any time prior to the Tender Clarification Deadline.

7.2 All questions/clarifications must be submitted via the Jaggaer e-sourcing system within the allotted timescale.

7.3 The Buyer will not enter into exclusive discussions regarding the requirements of this Further Competition with Potential Providers.

7.4 To ensure that all Potential Providers have equal access to information regarding this Further Competition, the Buyer will publish all its responses to questions raised by Potential Providers on an anonymous basis.

7.5 Responses will be published through the Jaggaer e-sourcing system by the allotted time.

7.6 At times the Buyer may issue communications about this tender through the Jaggaer e-sourcing system, therefore please ensure that you monitor the Jaggaer system on a regular basis.

8 Price

8.1 All SFIA pricing must be provided using the DSP pricing schedule provided within the tender pack. Pricing is based on SFIA rates of the roles specified on the DSP pricing schedule. You must also provide any offshore rates in the orange section of the pricing schedule

You must also provide transition costs on the Transition cost/Volume Discount template provided. In addition please provide details of any volume discount applicable in years 3 and 4 should DVSA utilise the options to extend the agreement.

9 Submitting a tender

9.1 All Tenders must be submitted through the Jaggaer e-sourcing system. You must submit your responses to the quality, social value and mandatory questions using the relevant “envelopes” in the Jaggaer system. Pricing must be provided using the price templates provided and submitted through the Jaggaer system.

9.2 A Tender must remain valid and capable of acceptance by the Buyer for a period of 90 days following the Tender Submission Deadline. A Tender with a shorter validity period may be rejected.

10 Tender Evaluation

10.1 Tenders will be evaluated in line with the Marking Scheme set out in Appendix C (Further Competition Questionnaire).

Criteria Number	Criteria	Percentage Weightings (or rank order of importance where applicable) To be set by the Buyer conducting the further competition - examples below (which in total should add up to 100%):
1	Quality and Social Value: (including delivery time, period of completion, sales service, good value). Please note that the Social Value question carries a 10% weighting.	75%
3	Price	25%

		(20% for SIIA pricing, 5% for transition costs)

10.2 Overall score

• The quality and price scores will be combined in the ratio 75:25 to provide an overall score.

• The bidder with the highest overall score will be awarded the contract - though DVSA reserves the right not to award a contract following the tender exercise.

10.3 All mandatory questions are evaluated on a pass/fail basis. If any mandatory question is answered "No" the tender will not be considered further. Please note that mandatory questions are not weighted. Technical/Service quality and Social Value questions will be evaluated against a pre-determined set of criteria and scored between 0 and 3 in accordance with the agreed criteria. Cost will be evaluated separately by a qualified Authority accountant. Please note that the "quality" and Social Value evaluation will be undertaken individually by each scoring member of the evaluation panel. Each individual evaluation will be sense checked by the Evaluation panel chair who must be a Senior Commercial manager to ensure the process has been followed correctly and fairly. A consensus meeting will then be held with all evaluation panel members to ensure that agreement is reached on the evaluation results. Once the evaluation has been completed, the relevant weighting will be applied and the supplier with the highest overall score will be offered the award.

10.4 Marking scheme for use in quality evaluation:

Marking scheme	Description
0	***Unanswered or totally inadequate response*** - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	***Minimal/partial Response*** - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance
2	***Good Response*** - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	***Excellent Response*** - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

10.5 The Total Score Available for each question set out in Appendix C (Further Competition Questionnaire) is as follows:

QUESTION	TOTAL SCORE AVAILABLE
Mandatory Questions [Please delete if not used and amend numbering in this table.]	Pass / Fail
Question 1	12%
Question 2	12%
Question 3	12%
Question 4	12%
Question 5	12%
Question 6 (Social Value)	12%
Question 7	12%
Question 8	16%
Price	25%

10.6 Overall score

• The quality and price scores will be combined in the ratio 75:25 to provide an overall score.

• The bidder with the highest overall score will be awarded the contract - though DVSA reserves the right not to award a contract following the tender exercise.

10.7 Costs

You must complete and submit the two cost templates provided with the tender pack (TTS CI and Legislative change pricing schedule and transition cost and volume discount pricing schedule).

11 Presentation

11.1 The top 3 scoring suppliers will be invited to give a presentation, specific details of which will be provided with the invitation. The presentation will not be scored but the content will be used to validate your written responses to the “Quality” questions. The presentation will be attended by the DVSA’s full evaluation panel and could result in the scoring applied against your answers being amended.

12 Contract Award

12.1 The Potential Provider that achieves the highest total score will be awarded the Contract.

12.2 If two or more Potential Providers obtain the highest total score, the Potential Provider with the highest score for the Quality/Social Value element of the tender evaluation will be deemed the winner and awarded the Contract.

12.3 If the Buyer receives only one Tender in relation to this Further Competition, the Potential Provider will be considered for the award of the Contract provided that they score a minimum of 2 against all Quality/Social Value questions.

13 Outcome Letters and Call-Off Contracts

13.1 Upon Contract Award Potential Providers will be notified of the tender outcome by Letter via the Jaggaer e-sourcing system.

APPENDIX A –TERMS OF THE FURTHER COMPETITION

14 Introduction

14.1 The Terms of the Further Competition regulate the conduct of the Potential Provider and the Buyer throughout the Further Competition. These terms also grant the Buyer specific rights and limit its liability.

14.2 In these Terms of the Further Competition any reference to 'person' includes, but is not limited to, any person, firm, body or association, corporate or incorporate.

15 Conduct

15.1 The Potential Provider agrees to abide by these Further Competition Terms and any instructions given in the Further Competition Invitation and agrees to ensure that any of its staff, contractors, subcontractors, consortium members and advisers involved or connected with the Further Competition abide by the same.

15.2 Contact and Canvassing During the Further Competition

15.2.1 The Potential Provider must not directly or indirectly canvass any Minister, public sector employee or agent regarding this Further Competition or attempt to procure any information from the same regarding the Further Competition (except where permitted by the Further Competition Invitation). Any attempt to do so may result in the Potential Provider’s disqualification from this Further Competition.

15.3 Collusive Behaviour

15.3.1 The Potential Provider must not (and shall ensure that its subcontractors, consortium members, advisors or companies within its Group do not):

15.3.2 fix or adjust any element of the Tender by agreement or arrangement with any other person;

15.3.3 communicate with any person other than the DVSA about the value, price or rates set out in the Tender; or information which would enable the precise or approximate value, price or rates to be calculated by any other person;

15.3.4 enter into any agreement or arrangement with any other person, so that person refrains from submitting a Tender;

15.3.5 share, permit or disclose to another person access to any information relating to the Tender (or another Tender to which it is party) with any other person;

15.3.6 offer or agree to pay, give or does pay, give any sum or sums of money, inducement or valuable consideration directly or indirectly to any other person, for doing or having done or causing or having caused to be done in relation to the Tender any other Tender or proposed Tender, any act or omission, except where such prohibited acts are undertaken with persons who are also participants in the Potential Provider's Tender, such as subcontractors, consortium members, advisors or companies within its group, or where disclosure to such person is made in confidence in order to obtain quotations necessary for the preparation of the Tender or obtain any necessary security.

15.3.7 If the Potential Provider breaches paragraph 2.2.1, the Buyer may (without prejudice to any other criminal or civil remedies available to it) disqualify the Potential Provider from further participation in the Further Competition.

15.3.8 The Buyer may require the Potential Provider to put in place any procedures or undertake any such action(s) that the Buyer in its sole discretion considers necessary to prevent or curtail any collusive behaviour.

16 Compliance

16.1 The Potential Provider agrees that in cases where their Tender is deemed non-compliant when compared with the requirements set out within the Invitation to Tender (e.g. budget, terms and conditions) they will be excluded from the Further Competition.

17 Right to cancel or vary the further competition

17.1 The Buyer reserves the right:

17.1.1 to amend, clarify, add to or withdraw all or any part of the Further Competition Invitation at any time during the Further Competition;

17.1.2 to vary any timetable or deadlines set out in the Further Competition Invitation;

17.1.3 not to conclude a contract for some or all of the goods and/or services (as applicable) for which Tenders are invited;

17.1.4 to cancel all or part of the Further Competition at any stage at any time.

17.2 The Potential Provider accepts and acknowledges that by issuing the Further Competition Invitation, the Buyer is not bound to accept a Tender or obliged to conclude a contract with the Potential Provider at all.

APPENDIX B – SPECIFICATION

18 Purpose

18.1 The Authority provides several digital services which are used by members of the public, MOT testers, licenced goods and passenger transport operators, and members of Authority staff involved in regulatory and administrative work.

18.2 These services support the Authority's core operations helping to meet its key objective of road safety. The scope of this contract is to provide CI and development for the Theory Test.

18.3 These teams are currently comprised of members of Authority staff, and team members from a contracted supplier. The team members work collaboratively to deliver outcomes defined within backlogs, owned, and prioritised by the Authority .

19 Background to the Contracting Authority

19.1 Driver and Vehicle Standards Agency (DVSA) is an executive agency of the Department for Transport.

19.2 We carry out driving tests, approve people to be driving instructors and MOT testers, carry out tests to make sure lorries and buses are safe to drive, carry out roadside checks on drivers and vehicles, and monitor vehicle recalls.

19.3 We're responsible for:

- carrying out theory tests and driving tests for people who want to drive cars, motorcycles, lorries, buses and coaches, and specialist vehicles.
- approving people to be driving instructors and motorcycle trainers and making sure they provide good quality training.
- approving people to be MOT testers, approving the centres they work in, and testing lorries, buses and coaches ourselves.
- carrying out roadside checks on commercial drivers to make sure they follow safety rules and keep their vehicles safe to drive.
- monitoring recalls of vehicles, parts and accessories to make sure that manufacturers fix problems quickly.
- approving training courses for qualified drivers, such as Driver Certificate of Professional Competence courses for lorry, bus and coach drivers, and drink-drive rehabilitation courses
- supporting the Traffic Commissioners for Great Britain and the Northern Ireland transport regulator to license and monitor companies who operate lorries, buses and coaches, and to register local bus services.

20 Specification

20.1 The Authority is looking to procure the services of a digital services delivery partner, to deliver continuous improvement outcomes for one of the Authority's suite of digital services and products, in line with Government Central Digital & Data Office (CDDO), formerly GDS, service standards.

20.2 Our definition of Continuous Improvement (CI) is detailed within this document.

20.3 The Authority provides several digital services which are used by members of the public, MOT testers, licenced goods and passenger transport operators, and members of Authority staff involved in regulatory and administrative work. These services support the Authority's core operations helping to meet its key objective of road safety.

20.4 This document sets out the Authority's requirement for the over-arching service to be delivered. Each request for the supplier to deliver the service will be in a specific Statement of Work.

20.5 For guidance, there are typical scenarios in which the Authority would use this contract.

- Deliver continuous improvement outcomes for the Theory Test digital services and products.
- Build the Theory digital services to our standards and technical specification requirements.
- To provide the service to enable the Authority to manage its priorities, for example to meet a legislative requirement.
- The supplier will work collaboratively with the Authority's Digital Services Department. This will allow the Authority flexibility to maintain continuous improvement of its digital services.

21 Continuous Improvement Definition

21.1 The Authority has identified eight key outcomes of Continuous Improvement (CI) and this contract will procure a service to enable delivery of those outcomes:

21.1.1 **Security:** Data secure and in line with GDPR; compliance maintained with Cabinet Office and National Cyber Security Centre (NCSC); end-to-end security protections from current and emerging threats with >10,000 attempts per week. Just because a service is secure today does not mean it will be secure tomorrow. A key outcome is ensuring that a service is able to maintain authority to operate. Additional security requirements detailed in Section 35.

21.1.2 **Data:** Ensure data is accurate and readily retrievable to support Authority needs and operations/enforcement.

21.1.3 **Availability, Scalability and Stability:** Service is reliable, scaled to meet demand, with a remediation approach to issues – and to reduce risk of system failures.

21.1.4 **Currency and Operability:** Software versions are up to date, with patching and maintenance – and to reduce risk of system failures.

21.1.5 **Responsiveness, Adaptability, and Accessibility:** Service works on all modern devices and software, and in line with emergent regulations such as for accessibility and cookies.

21.1.6 **Cost Optimisation of Cloud Platforms:** Architecture enhancements to stay aligned to Cloud developments – and to enable access to favourable commercial trading options for usage.

21.1.7 **Developing the Service:** Meeting new policy, business and user needs to best meet policy objectives – and based on ongoing user research, feedback, and performance analysis.

21.1.8 **Economies of Scale:** Working across Digital Services, the wider Agency and CDDO to identify opportunities for alignment, such as end-to-end user journeys, common architecture and design patterns, shared functionality and CDDO services such as payments.

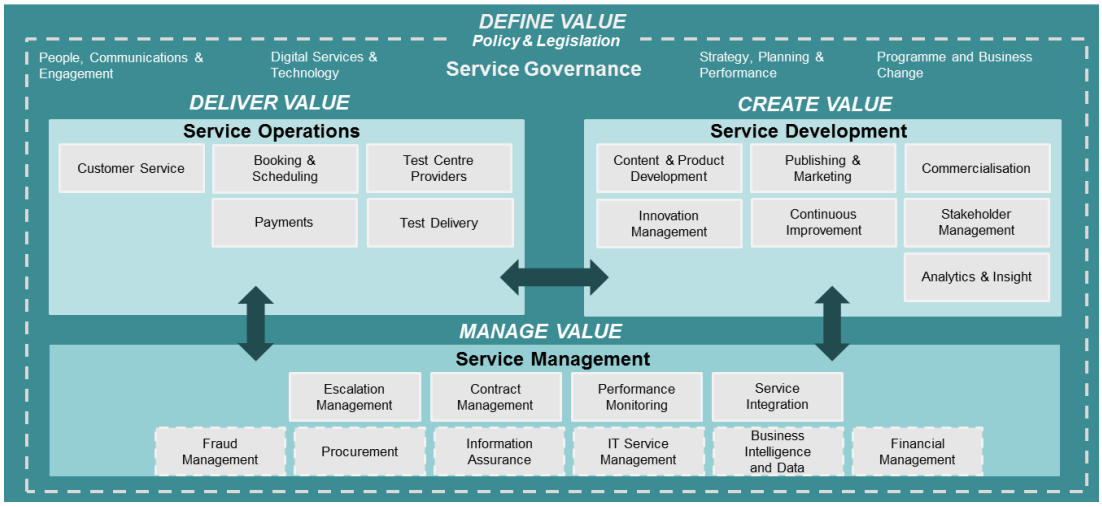
21.1.9 **Quality of Delivery**: All deliveries will encompass evidence based quality processes and use of embedded tools as a core part of the delivery. Quality processes will reviewed and updated as part of the continuous improvement

22 The Theory Test service

22.1 Target Operating Model

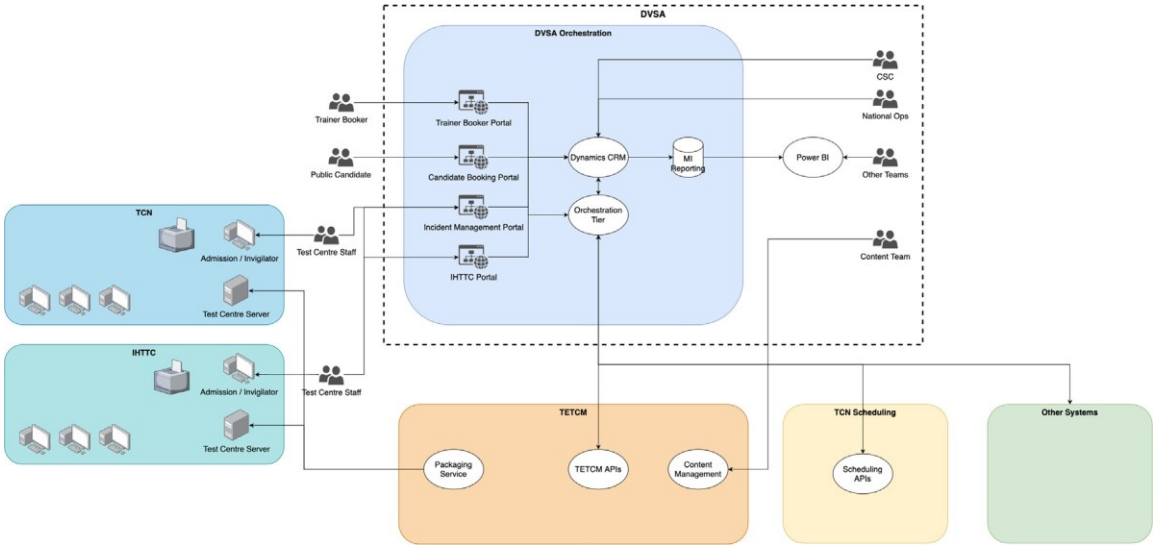
22.1.1 To achieve the Theory Test vision, the operating model has been designed around three broad components which, when combined, delivers the overall service to Business Customers and Candidates:

Service Operations – responsible for delivering the front-end testing services to the Business Customers and Candidates to continue delivering high standards and quality.
Service Development – responsible for the development and implementation of learning and test content, as well as continuously developing the quality of the TTS whilst ensure alignment and consistency of products.
Service Management – responsible for managing the overall delivery of the TTS using performance data and analytics.



22.2 High level architecture

22.2.1 The Theory Test service comprises the following services:



22.2.2 Orchestration encompasses several distinct high-level components namely; integration layer, CRM, Data Repository, reporting interfaces and system logic components. Separate internal systems and third-party systems will need to interface with the platform through the integration layer, making the systems available to internal components.

22.2.3 CRM platform provides several workflow processes to facilitate the running of the service. Users for the workflows will include citizens, internal Authority staff and third-party suppliers.

22.2.4 The Authority maintains integrity and ownership of the data across different parts of the service. The transactional data is persisted within the CRM system with the long-term (anonymised / aggregated) data and metric data being persisted within the Data Repository.

22.2.5 Reporting and analytics are generated across the service to provide insights relating to KPIs and SLAs for all aspects of the TTS. This will include information provided by 3rd party suppliers which is aggregated to support the relevant reports.

22.2.6 The table below provides a description of the containers and components identified in the target architecture in relation to the work the Potential Provider is required to carry out.

22.2.7 the TTS overall IT system delivers an Authority function for orchestration, which is responsible for:

- Managing business processes/workflows through the CRM.
- Managing the design and storage of data within the CRM.

- Managing the integrations to other systems (internal to the Authority and external) through configuration of the integration layer.
- Logic – includes process to 'move' data around the platform between for example; the CRM and Data Repository, the CRM and the TETCM.
- Managing the Reporting and Analytic through dashboards and reports

Container Name	Responsibilities
TETCM (Test Engine / Test Content Management System)	The TETCM is responsible for: Providing a facility for the Authority to add and manage the test content Providing the Software to admit candidates into the Test Centres Providing the Software which runs on the workstations Providing Software to support Test Control, Test Generation, Invigilation, Test Feedback and Test Results
TCN (Test Centre Network)	The TCN is responsible for: Providing the slot availability within each provider's TCN to support the online booking process ("Scheduling") Access to Scheduling system interface Providing Test Centre Information Providing staff and premises
Data Repository	The Data Repository is an export of MI data from the transactional system, which can then be used for other purposes, e.g. audit, reporting etc.
DVLA	DVLA integration is responsible for confirming candidate eligibility
Authority	The Authority's integration team is responsible for: Taking payments from the candidate / business (CPMS) Customer Payment Management System Finance and reconciliation (utilising SAP via shared service partner) Informing the Authority practical test booking system (TARS) Identity and access management ("Active Directory")
DVA	DVA integration is for Northern Ireland test takers and is responsible for: Candidate eligibility Storing results
Gov UK	Gov UK provide a number of Gov-Platform-As-A-Service (GPaaS) integrations, and will be responsible for: The static web content which will be used on the static pages of Gov UK for the theory test (Gov CMS) Notifying candidates by email/text (Notify) of their booking and/or reminder.
Other 3rd Party Services	Any other 3rd Party integrations that are currently known: Geo Location Search, which will be used as part of the booking process

22.2.8 The prioritised backlog is comprised of Stories (and bugs, spikes, tasks etc.) from different user perspectives across the different Continuous Improvement services.

22.2.9 More information on Agile delivery, principles, tools and governance can be found at: https://www.gov.uk/service-manual/agile-delivery

23 Individual Technology Stacks

23.1 **CRM -** Dynamics CE (Customer Engagement) foundation extended and augmented as part of a more comprehensive Power Platform Solution (Power Apps, Power Automate, Dataverse).

23.2 **Candidate Booking Portal -** Serverless web application built on Azure Functions (Typescript/node.js), Express, Nunjucks, HTML, SASS, Redis (sessions).

23.3 **Trainer Booker Portal, IHTTC Portal, Incident Management Portal -** 3 different PowerApp Portals with the Dataverse from the Dynamics / CRM as the source. 2 of the Portals are government styled and assessed and the IM Portal is a customised version of the MS Case Management template.

23.4 **Orchestration Tier** Serverless integration tier (REST APIs and SFTP/File transfer) built on Azure APIM, Functions (Typescript/node.js), OpenAPI/REST, Cosmos, Redis, Containers

23.5 **Data Analytics & MI -** Data pipelines and reporting DB built using Python, Synapse Link for Dataverse, Data Lake Storage, Azure SQL, DataBricks, Flyway, consumed by PowerBI.

24 CI Delivery Outcomes

24.1 CI delivery outcomes are defined in the product roadmap. A product Backlog will be defined, refined and prioritised in conjunction with the Authority. The delivery outcomes for each sprint will be jointly agreed and delivered to the expected quality with the agreed documentation

25 Services Provided to Deliver the Outcomes

Supplier capabilities will include the following skillsets

- Delivery Management
- Business Analysis
- Service Design
- Content Design
- User Research
- Architecture
- Software Development
- Quality Assurance and Test Management
- Performance Analysis
- Information Security
- Release Management

26 Responsibilities

26.1 Authority responsibilities

26.2 The Authority will retain ownership and responsibility for maintaining its strategies and policies for:

- Architecture
- Technology
- Security
- Data Protection

26.3 The Authority will retain ownership of a number of corporate responsibilities. These are included in, but not limited to the list below, and may change during the course of the contract:

- Initiation of all work, governance, approvals, and funding processes.
- Strategy, and policies.
- All data within the systems worked on by the supplier.
- All Intellectual Property Rights.
- All data will be hosted on Authority systems in accordance with all appropriate security and data protection policies as directed by the Authority.
- The Authority will be responsible for maintaining oversight of all work carried out by the supplier.

26.4 A number of items will be worked on collaboratively between the Authority and supplier. The supplier will be responsible for providing expertise and solutions within the agreed frameworks, joint working and collaboration will be key to the success. Authority governance processes will approve solutions and maintain overall ownership. These items are included in, but not limited to the list below, and may change during the course of the contract:

- All roadmaps for development.
- A prioritised backlog of work for the Theory Test digital service.
- All processes/ways of working.
- Objectives, delivery performance, specification of work.

27 Business Requirements

27.1 To provide services for software development and delivery. Based on agreed roadmaps, sprint plans and defined outcomes

27.2 This work will deliver, security and stability, bug fixes and new enhancements ensuring technical currency of the existing digital services.

27.3 The supplier will deliver against the jointly agreed prioritised backlogs of work for the Theory Test service. The backlog will include CI backlogs; deliver new features based on user feedback, operability, technical currency or to support Policy change, and result in technically current services that are secure, maintainable, and extensible.

27.4 Where new features or updates to functionality are being introduced, training material may need to be provided to support a smooth implementation within the Authority. The requirements for training materials will be agreed between the Authority and Supplier as part of the product planning.

27.5 Collaboration - Supplier shall work collaboratively with and support the Authority and its other suppliers (e.g. TCN, TETCM, Technical Support Services, DVLA, DVA, Capita, CCDO) to ensure the successful delivery of all services related to the TTS. This applies to all elements of the TTS, from development, testing, integration, quality assurance and ensuring plans are coherent, transparent and exhaustive. Any stakeholder engagement requirements would be clear as part of the planning process. It will also include analysis and assistance on incidents where requested by the Authority or Technical Support Services.

27.6 The Supplier shall work collaboratively with the Authority to ensure suitable skills and knowledge transfer to the Authority's staff in order help to identify and build opportunities for in house capability where appropriate.

27.7 In order to ensure the effective delivery of the Authority's objectives, a number of required behaviours have been outlined. The Supplier will act in the following ways:

27.7.1 **Collaborative Intention:** the Supplier must act in good faith and adopt and maintain a genuine non-defensive presence and make a commitment to mutual success in its relationship with the Authority and the TTS Suppliers;

27.7.2 **Openness:** the Supplier must be honest in its dealings and open to honest feedback and create a culture of openness that allows all of the Supplier, the TTS Suppliers and the Authority to feel safe enough to discuss concerns, solve problems and deal directly with difficult issues;

27.7.3 **Self Accountability:** the Supplier must behave in a fair and reasonable manner and must take responsibility for its circumstances and the choices it makes either through its action or failing to act as well as the intended and unforeseen consequences of these actions. The Supplier must focus on the solution to a problem or issue rather than seeking to blame the Authority or any TTS Supplier;

27.7.4 **Self-Awareness and Awareness of Others:** the Supplier must commit to understanding its own organisations and issues within its own organisations as well as understanding concerns, intentions and motivations of the Authority and the TTS Suppliers as well as the culture and context of the Authority and the TTS Suppliers' circumstances;

27.7.5 **Problem Solving and Negotiating:** the Supplier must proactively use problem-solving methods that promote a collaborative and co-operative atmosphere and avoid fostering covert, overt, conscious or unconscious enmity, conflicts or point-scoring;

27.7.6 **Expertise:** the Supplier shall commit to using its expertise to the benefit of the overall Theory Test Service and the end-to-end services delivered to the Authority and the Service Beneficiaries. The Supplier shall ensure that the Supplier Personnel work collaboratively with FTTS Supplier personnel, laying aside considerations of individual competitive advantage in the interests of the Authority;

27.7.7 **Promote Value:** the Supplier shall demonstrate a preparedness to innovate and adopt best practises and be forthcoming in initiating proposals for new best practices which deliver improved value to the Authority and the Service Beneficiaries;

27.7.8 **Forward Looking:** the Supplier shall take a forward looking approach that does not dwell on past issues or conflicts of delivery methods, other than ensuring that past lessons are learnt so as to maximise the effective delivery of end-to-end services to the Authority and the Service Beneficiaries;

27.8 **Quality assurance requirements**

27.8.1 This section deals with quality assurance requirements that the Supplier must deliver during the period of the Contract.

27.8.2 The Supplier will ensure that all quotations are accurate and reasonable for time and money.

27.8.3 The Supplier will utilise their expertise, skills and knowledge to make recommendations, where necessary, to the Authority. This will include any third party product recommendations.

27.8.4 Following a Continuous Integration and delivery approach, it is intended that there will be incremental releases of functionality to a production (live) environment. The Authority will specify criteria for the acceptance of these releases and the Supplier staff will need to work with Authority and their support partners to ensure that these are met.

27.8.5 The Authority expects that the Supplier shall actively support each release of new functionality and will provide the immediate response to any critical and high severity defects identified within the agreed warranty period (see clause 12.4). Thereafter, responsibility will be passed to the Authority function and their support partners.

27.8.6 Quality of software delivery is essential for the Theory Test. The Supplier will warranty all software delivered into the production (live) environment for a period of 4 weeks after deployment to production. If a software bug / error is identified during this 4 week period, the Supplier will remediate at their own cost with no costs to the Authority.

27.8.7 Bugs/Errors identified by the Authority will have a root cause analysis undertaken by the supplier, which confirms both how the defect was introduced and how the bug was released through the quality process.

27.8.8 Acceptance criteria covering both functional and non-functional elements will be defined in advance for each item of work, which is aligned to an agreed ‘Definition of Ready’ and approved by DVSA Product Owners.

27.8.9 Analysis expertise will help define value and benefit for each piece of work in accordance with the agreed 'Definition of Ready'.

27.8.10 Items of work will be delivered to an agreed 'Definition of Done'.

27.8.11 Test evidence for sign-off is provided by the supplier in business oriented terms or technical assurance is provided by the supplier.

27.8.12 Production of regular quality assessment reports will be provided, indicating how continuous improvements to quality processes can further improve. Additional actions for improvements will be centrally tracked and reported.

27.8.13 Performance of the contract will be managed by the Supplier delivery manager. They will work closely with the Authority service owner. There will be regular joint reviews against work in progress.

These reviews of progress will include, but not limited to:

- Tracking progress against roadmap plans and roadmaps
- Use of a timeboxed approach to delivery – to demonstrate completion to plan.
- Service management boards
- Review of risk/issues/decisions and dependencies (RAIDD) and escalation if necessary
- Emerging findings
- Costs incurred (running total)
- Review of upcoming work/next steps
- Review of resources
- Timescales for delivery – ensuring work is progressing to plan

27.8.14 The Authority follows the GDS Design Principles and Digital Service Standard to deliver public facing digital services, outlining the principles applied, methods adopted and ability to deliver successful outcomes.

CDDO Design Principles information can be found at:
https://www.gov.uk/guidance/government-design-principles

CDDO Service Standard information can be found at:
https://www.gov.uk/service-manual/service-standard

28 Technical Requirements

28.1 Suppliers will need to have experience in those technologies outlined below:

28.2 **Microsoft Dynamics 365 technologies – not limited to but includes**

Microsoft Dynamics 365 technologies (including Dynamics for Customer Engagement), Microsoft Power Platform (including Dataverse, CDM, Apps, Automate, BI), C#, PowerApp Portals (Power Pages)

28.3 **Microsoft Azure technologies – not limited to but includes**

DNS Zone, Front Door, WAF, CDN, Vnets, Functions, Redis Cache, Service Bus, APIM, Key Vault, AppInsights, AAD (B2B and B2C), Containers, Cosmos, SQL, Storage – File/Blob/Data Lake, Synapse Link for Dataverse

28.4 **General Infrastructure Tools and Infra as Code Tooling**

Azure DevOps – pipelines, repositories, artifacts, GitHub, SonarQube, ARM templates, Powershell, Terraform, Docker, Incapsula Imperva, AlertLogic.

28.5 **Production code:**

C#, Typescript

28.6 **Testing (Including automation):**

Typescript/Jest, C#/xUnit, EasyRepro, JMeter, Postman, TestCafe/BrowserStack, SpecFlow/Selenium

29 Availability

29.1 Services must remain highly available, secure, resilient, and technically current whilst built upon.

30 Authority Teams and Ways of Working

30.1 **Existing Authority Team**

The Authority currently has these permanent roles within the Theory Test department:

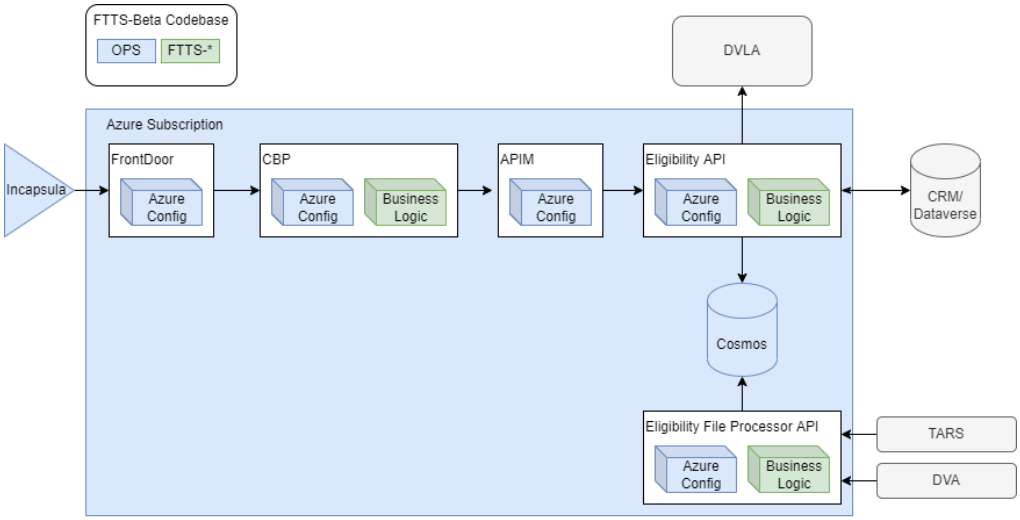
- Information Security analysts
- Service Owner
- Product Owner
- Technical Architect
- Reporting Analysts
- Business Analyst (Apprenticeship)
- Test Manager (Apprenticeship)

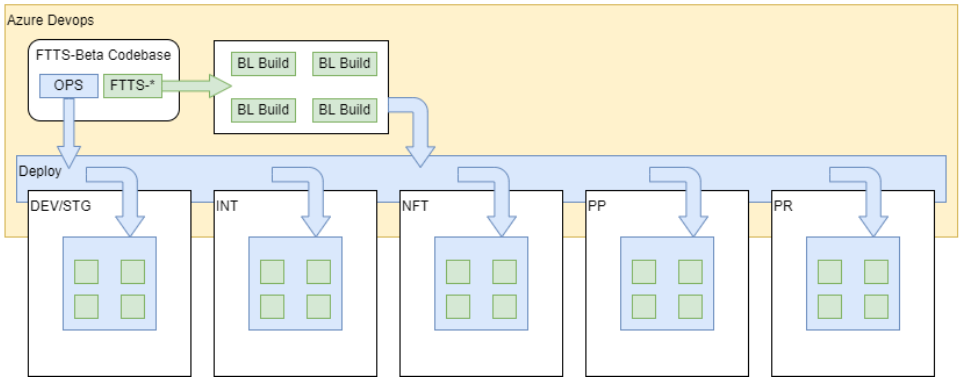
30.2 **Technical Support Services (TSS)**

30.2.1 The Authority contracts a third party to provide technical support to the theory test taking total responsibility for the management of Theory Test services within the Azure production tenancy.

30.2.2 The scope of TSS is:

- Maintenance, improvements and security of deployment pipelines and deployment release process for all Azure and CRM components and supporting infrastructure and environments (nonproduction and production environments)
- Maturing relationship with Authority Cloud Infrastructure to implement Azure AD underpinnings for FTTS in line with overall Authority Azure Cloud Strategy
- Progressing feature work infrastructure dependency changes in line with CI sprint timescales.
- Accountable for the definition of deployment pipeline for all integrated environments (ops directory).
- Development, maintenance, improvements and security of MI and Data Reporting Service





31 Business Location

31.1 The Authority is working on a 'hybrid' model with staff working at a combination of office locations and from other suitable locations.

31.2 The Authority would accept a similar arrangement for supplier staff. Supplier staff may be required to work collaboratively with staff at Authority locations, with the remainder of the work being carried out remotely.

31.3 Remote working would be conducted using collaboration software that is available for Authority staff and any artefacts produced will be in formats that are usable by Authority staff**.**

31.4 The Authority mandates the use of the Atlassian (JIRA/Confluence) software for digital delivery

31.5 Key personnel will be required to attend in person for service management boards.

31.6 Supplier will demonstrate successful management of their staff working remotely.

31.7 The Authority key business location for this work is:

Unity Square, Nottingham NG2 1AW.

31.8 Travel to other locations may be required.

31.9 In order to provide analysis and assistance on incidents where requested by the Authority or Technical Support Services (clause 27.4), the Supplier must provide appropriately skilled staff who are located in the UK. These staff may be granted access to production data subject to appropriate security clearance to be agreed with DVSA.

32 Business Continuity

32.1 In the event of a major business interruption affecting the supplier, we expect the Supplier to understand what their critical activities are in supporting the Authority, maintaining the capability to resume operations within agreed timeframes to ensure they provide an adequate service to the Authority. The Supplier will aim to minimise impacts using a focused, well managed response process and effective communications should a disruptive incident occur.

32.2 The Supplier will develop their own business continuity plan to support the overall Theory Test business continuity strategy.

32.3 In the event of a major business interruption the Supplier will deploy the required resources to implement their Business Continuity Plan. The Supplier will respond to the needs of the customer even if that means a potential reduction in normal service levels.

32.4 The Supplier will maintain a regular business continuity plan review process and will inform the Authority of any changes and/or improvements arising from this review.

32.5 The supplier will be required to take part in wider service business continuity testing and address actions from lessons learnt where required.

33 Business Hours

33.1 The Authority's business hours are 0700 – 1900 Monday to Friday excluding Bank Holidays in England.

33.2 As part of this contract the Supplier staff will be expected to support out of working hours software releases where required.

34 Security

34.1 **Security Overview**

34.1.1 The Supplier must consider security and privacy throughout the entire TTS Service solution lifecycle, including architecture and design, development, deployment and live operation processes where these are delivered under this Contract.

34.1.2 The Supplier shall ensure the TTS Service CI activities as delivered under this contract maintain the current level of security protection, which is audited to ISO 27001 and utilises a maturing suite of procedural and technical security controls

34.1.3 The Supplier (and subcontractors) shall meet the relevant clauses of the long form DSP Security Schedule (Call-Off Schedule 9 Security) during its fulfilment of the requirements of the Contract and the Security Management Plan must include but not be limited to the Delivery Partner's commitment to:

- Security Governance
- Compliance with relevant legislation
- Personnel security
- Physical security of any supplier premises used to host DVSA data, code or artefacts
- IT Security including where DVSA data, code or artefacts are held on the supplier's ICT system(s)
- Secure data transfer mechanisms
- Incident management
- Security testing
- Audit requirements including audit by the DVSA as required

34.2 **Security standards**

34.2.1 The supplier (and any subcontractors used to deliver tasks under this Contract) must hold the following security certifications with the scope of certification fully covering the delivery of the services under this Contract:

- ISO27001 from a UKAS certifying body
- Cyber Essentials Plus

34.2.2 All work undertaken under the contract and solutions delivered must be compliant with/or aligns to the following industry and HMG standards:

- AWS and Microsoft best security practice where relevant
- NCSC Guidance and Principles
- NIST security and cybersecurity standards
- DVSA security policies (as provided)

- DPA2018 and GDPR for handling personal data
- General security good practice including but not limited to for example: management of secrets, management of vulnerabilities, auditing.

34.3 **Security Governance**

34.3.1 The Supplier shall contribute to the security governance of the TTS service by:

- Attending the Orchestration monthly Security Working Group meetings plus other security meetings as requested by DVSA
- Providing written/verbal contributions as requested by DVSA
- Liaising with other internal DVSA system representatives, projects and third-party suppliers as requested by DVSA
- Contribute to assessment of solution compliance with NIST standards
- Providing a suitably qualified single security point of contact for DVSA who will attend meetings and provide liaison.
- Security Artefacts

34.3.2 The Supplier must create or maintain suitable documentation to support the maintenance of a secure TTS solution and maintain DVSA Authority to Operate (ATO) such as (but not limited to):

- Risk and impact assessments
- Data Protection Impact Assessment and updates (where requested by DVSA)
- Technical security architecture (s)
- High Level Designs (HLDs)
- Low level designs/configurations
- Security Assurance Documentation
- Change documentation
- Release documentation
- JIRA tickets relating to security
- Security testing scopes
- Security testing reports
- Security testing remediation plans
- Security management processes/guidance
- Security procedures

34.3.3 Artefacts must be kept up to date with agreed changes to the solution and services delivered under this Contract and must be reviewed for currency not less than quarterly.

34.4 **Security risk management**

34.4.1 The Supplier must ensure that the secure delivery of the services within this Contract continues to mitigate against the key risks to DVSA including (but not limited to):

- Loss of DVSA personal data
- Loss/compromise of proprietary material
- Unauthorised access to DVSA data
- Non-repudiation of processing activity
- Overall integrity of the DVSA Theory Test service and testing process
- Availability of the existing DVSA Theory Test service and testing
- Other connected DVSA and partner organisation services

34.5 **Data Protection**

34.5.1 Delivery of this contract might require the supplier (or their subcontractors where specifically agreed with DVSA) to process Personal Data (as defined in the GDPR) on the DVSA's behalf.

34.5.2 The DVSA will be the Data Controller and the supplier will act as the Data Processor.

34.5.3 The supplier must process Personal Data only on the DVSA's documented instructions, as set out in DSP Joint Schedule 11 (Processing Data) of the Contract and be subject to the full legal requirements placed upon them by GDPR.

34.6 **Offshoring**

34.6.1 The DVSA preference is for onshore arrangements to be in place.

34.6.2 DVSA may choose to consider proposals including offshoring whether inside the EEA or beyond. Any proposal should include sufficient information to address the risks that DVSA would be looking to mitigate as part of such a solution. For example:

- The country in which the data is to be processed needs to have a UK adequacy decision in place or where this is not the case, other control measures are in place such as standard contractual clauses.
- Local laws and statutes may oblige organisations to provide access to DVSA data (including personal data and data relating to the security of DVSA systems) due to the processing happening in that country. If it's an EU member state, we may be required to have a representative and a Data Protection Officer based within that country.
- Additional mitigations for where there aren't equivalent standards e.g.
    - Physical security of the sites being used to house resource or data for the contract.
    - Vetting in the country of employment for resource.
- Information about DVSA and access to DVSA systems are shared or accessed more widely that just the personnel working on the DVSA account.
- Any changes to data being handled must be notified to, and agreed with, DVSA in advance. This includes the access of non-personal data from outside the UK.

34.6.3 If the proposal includes offshoring as part of the proposal, costs for DVSA to assure proposed arrangements should be included in the proposed costs. A minimum of one visit every 2 years to the proposed sites by 2 individuals should be included.

34.6.4 Offshoring means:

- the actual data being handled or processed outside the UK.
- a backup copy of the data being handled or processed outside the UK.
- IT support being able to access the data from outside the UK.

34.6.5 This also applies to any sub-contractors.

34.7 **Toolsets and environments**

34.7.1 The Supplier must provide suitable controls and assurance of the tools used to deliver the contract including any development processes and environments such that:

- Only assured tools as agreed with the DVSA are used to process DVSA data and artefacts
- Access to any development and testing environments is controlled with auditable access controls lists, with formal auditable onboarding and offboarding processes and records
- Devices allowed to access the development and testing environments must comply with NCSC guidance for End User Devices as a minimum standard.
- Configuration control of development and testing environments is maintained and suitable monitoring of activity is carried out
- Personal data is not used for testing or demonstration purposes unless suitably obfuscated and agreed with the DVSA

34.8 **Security Testing**

34.8.1 The Supplier must arrange for an IT Health Check for the Supplier System in any of the following circumstances:

- Prior to a grant of Authority to Proceed or Authority to Operate (e.g. events where the Supplier developed components or solutions are connected to the existing TTS services or external systems, loaded with Real Data or prior to live operation);
- As part of the DVSA Security Assurance process integral to change management. Whenever any change is being planned for the existing TTS system that is assessed by the Change process as significantly impacting security, whether it relates to business processes, software, infrastructure or ICT support processes. This includes significant releases in an Agile development.
- Periodically, defined by risk, but generally at not more than 12-month intervals

34.8.2 The ITHC must be performed by a NCSC Green-light CHECK or CREST approved supplier

The Supplier must document and share with DVSA:

- ITHC scopes
- ITHC results
- Identified vulnerabilities
- Evidence for remediation

34.8.3 DVSA must be given the opportunity to approve any ITHC scopes in a timely manner prior to testing and attend daily feedback meetings as requested with the ITHC testing team

34.8.4 The Supplier shall ensure that ITHC observations are addressed by either:

- Mitigating vulnerabilities in a timely manner as agreed with DVSA;
- Obtaining formal acceptance of the vulnerability by DVSA

34.9 **Security Audit**

34.9.1 The Supplier must facilitate the DVSA to carry out security audits on its estate (and those of its subcontractors) where used to directly or indirectly deliver the services to the DVSA, including immediately without prior arrangement in response to a security alert or incident.

34.9.2 DVSA security audits will be agreed between the DVSA and the Supplier, and carefully planned to minimise disruptions to business processes.

34.10 **Security training and awareness**

34.10.1 The Supplier must ensure that its personnel go through regular mandatory data handling, data protection, cyber security awareness, and incident handling training to understand what an incident is, and how they should report it using the Supplier's incident handling processes. Training must inform users of good security practices, such as locking their computer, not using untrusted USB devices etc

34.11 **Security Incident Management**

34.11.1 The Supplier must have an incident handling approach that is able to align with the DVSA's extant processes. The Supplier must ensure that any necessary people, data and systems are made available to the DVSA to support the handling, resolution and investigation of an incident.

34.11.2 An incident is any event or action that breaches information security policies and procedures or which compromises, or threatens to compromise, the confidentiality, integrity or availability of information, assets, the communications infrastructure or IT equipment that is being used by the Supplier and their contractors to deliver the services under this contract to DVSA.

Incidents include, but aren't limited to:

- breaches of physical security.
- detection or introduction of malicious code.
- inappropriate content.
- inappropriate or unauthorised access of IT services or information.
- malfunctions of software.
- misuse of information, items and/or equipment.
- theft or loss of information, items and/or equipment.
- unauthorised destruction of information.
- unauthorised disclosure of information.
- uncontrolled system changes.
- unsecure information, items and/or equipment.
- violations of network and system access.

34.11.3 The Supplier must inform the DVSA as soon as possible of observing an incident (including weekends and weekdays, public holidays).

34.11.4 The Supplier must assist the DVSA in determining and implementing measures and processes to handle an incident. The DVSA will assess incidents and determine if they are to be classified as near misses, security weaknesses or incidents and what actions, if any, are to be taken to mitigate them.

34.12 **Security Clearance**

34.12.1 For all individuals (including subcontractors) a Baseline Personnel Security Standard (BPSS) must be undertaken for their staff before they begin working on this contract.

Details of which can be found here:

https://www.gov.uk/government/publications/unitedkingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels.

34.12.2 For any individuals offshore a BPSS equivalent must be agreed with DVSA and undertaken.

34.12.3 DVSA and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable DVSA to determine which roles require additional vetting such as a specific National Security vetting clearance (e.g. a Counter Terrorist Check; a Security Check).

34.12.4 Roles which are likely to require additional vetting include system administrators, security team members, developers and system architects whose role would provide those individuals with privileged access to IT systems which process large volumes of personal data, security data or data which is classified as OFFICIAL-SENSITIVE

34.12.5 Any individuals requiring additional clearances as agreed with DVSA must have completed the vetting process prior to access being granted.

34.12.6 Suppliers are responsible for ensuring that any required additional clearances remain throughout an individuals involvement in this contract

34.12.7 Suppliers are responsible for ensuring that suitable cleared personnel are available to fulfil roles (as per paragraph 34.12.5) that are reasonably expected in delivery of the contract.

34.13 **Data Deletion**

34.13.1 During the contract the supplier and any relevant subcontractors must:

- securely erase any or all DVSA Data held by the Supplier when requested to do so by the DVSA; and
- securely destroy all media that has held DVSA Data at the end of life of that media in accordance with any specific requirements in the Contract and, in the absence of any such requirements, as directed by the DVSA
- securely destroy DVSA Data only on sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001; and
- are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the DVSA

35 Social Value

35.1 In September 2020, the Government implemented measures to promote new jobs and skills, encourage economic growth and prosperity, tackle climate change and level up the UK. Social value is included in the procurement model and will be used by government departments to assess a supplier's social impact.

35.2 This approach will mean more opportunities for SMEs and social enterprises to win Government contracts by demonstrating the full extent of the value they would generate.

35.3 Value for money will still be paramount, but a bidder's social value score will be incorporated into assessment of contracts.

35.4 Government departments will use the social value model to assess and score suppliers on the wider positive benefits they bring by delivering the contract. This will mean that value for money for the taxpayer can be maximised while also building a more resilient and diverse supplier base.

35.5 The social value model, which departments will assess contracts on, includes:

- Supporting COVID-19 recovery, including helping local communities manage and recover from the impact of COVID;
- Tackling economic inequality, including creating new businesses, jobs and skills, as well as increasing supply chain resilience;
- Fighting climate change and reducing waste;
- Driving equal opportunity, including reducing the disability employment gap and tackling workforce inequality Improving health and wellbeing and community integration.

35.6 This approach will apply tests that all bidders, irrespective of their size and type, will be capable of meeting and therefore further levels the playing field for the UK's small businesses, start-ups and voluntary and community sector organisations and social enterprises.

35.7 The Authority will be assessing evidence of how suppliers are driving equal opportunity by tackling workforce inequality.

35.8 All Potential Providers are required to include within their response to tender evidence of how they create opportunities to tackle training, employment, skills and pay inequality in the contract workforce, or to support in-work progression to help people in the contract workforce to move into higher paid work by developing new skills relevant to the contract.

35.9 **To note:** It is a legal requirement for companies with 250 employees or more to publish their annual gender pay data on-line.

35.10 The Authority has selected this criterion as relevant to underpinning the delivery of services within the contract, and as being aligned to its own equal opportunities and inclusion policies.

35.11 More information about the Social Value Model used for government procurement is at:

https://www.gov.uk/government/news/new-measures-to-deliver-value-to-society-through-public-procurement

36 Skills and experience

36.1 **Essential Skills and Experience**

- The Authority will use the listed skills and experience to help them evaluate suppliers' technical competence.

36.2 **Software Development**

- Experience of full software development lifecycle
- Experience of REST API design.
- Expertise with developer best practice including pair programming, code reviews, TDD.
- Experience of developing in Microsoft Azure cloud-based digital services at scale.
- Experience with Runtimes and Languages: C#, Typescript, Node.js.
- Experience with web frameworks – particularly Node Express
- Experience of Microsoft Dynamics and Power Platform technologies, including customisation/plugins/extensions, use of low-code solutions, and automation of testing and deployment to enable continuous integration
- Experience of Version control systems: Git, (Azure DevOps, Github)
- Knowledge of distributed systems.
- Knowledge of relational database technologies (e.g., Azure SQL).
- Knowledge of No-SQL storage systems (e.g., Cosmos DB)
- Awareness of public sector work e.g., UK Government CDDO.
- Experience working with Azure managed Services, Front Door, WAF, CDN, VNets, Functions, Redis Cache, Service Bus, APIM, Key Vault, AppInsights, AAD (B2B and B2C), Containers, Storage – File/Blob/Data Lake.
- Experience with general Infrastructure tools and Infra as code tooling: Azure DevOps pipelines, ARM templates.
- Awareness of NCSC cloud security principles for service security.
- Experience of OWASP Application Security Verification Standard for application development and testing.
- Awareness of static analysis tools and code quality tooling
- Awareness of Semantic and Accessibility Web Standards (W3C, WCAG)

36.3 **Software Testing**

- Experience with Automated testing and test engineering in an Agile environment
- Experience in forming and following test plans and strategies
- Experience of non-functional testing and tooling
- Experience of API and Microservices Architecture testing
- Experience of Performance and load testing, and creating representative performance test scenarios from measured production end user behaviour
- Experience of Typescript, Jest, TestCafe, BrowserStack, Postman, and other automated testing tools
- Experience with automating the regression testing of Microsoft Dynamics/Power Platform and low-code solutions
- Experience with JMeter and other performance testing tools
- Experience with Docker

- Experience of Version control systems: Git, (Azure DevOps, Github)
- Experience of CI / CD tooling: Azure DevOps pipelines

36.4 **Architecture**

- Significant and proven experience of architecting highly available, fault tolerant solutions on Microsoft Azure.
- Deep understanding and experience of various software architectures (Serverless and Microservices) and methodologies
- Deep understanding and experience of various Microsoft Dynamics and Power Platform technologies, including customisation/plugins/extensions, use of low-code solutions, and automation of testing and deployment to enable continuous integration
- Fluent in architectural design techniques with experience of facilitating development of architectural plans.
- Great at documenting your solutions in a way that varied audience can understand.
- Experience of emergent architecture and shared services patterns.
- Experience with managing technical debt

36.5 **Data**

- Relational database services (both relational and non-relational or NoSQL) within cloud providers
- Experience with Data Lake architectures and real-time data pipelines hosted in Microsoft Azure
- Experience with cloud-based recovery strategies
- Experience with both support and design
- Experience and understanding of database design and how this is impacted by usage
- Experience of monitoring strategies within a cloud environment
- Experience with DB performance tuning, query optimisation and troubleshooting
- Experience and knowledge of mitigation strategies during change

36.6 **Delivery Management**

- Skills and experience in delivery roles consistent with the technologies (listed above) to deliver large scale cloud-based digital services.
- Experience of agile delivery.
- Version control.
- Experience with developing CI/CD delivery pipelines.
- Experience with managing technical debt
- Experience in documenting technical solutions so that they are understood by a wide range of readers (e.g., non-technical staff).

36.7 **Service Design**

- Experienced with Service Design including problem framing, customer journey mapping, service blueprinting, end to end service mapping, and facilitation of multiple stakeholders in meetings and workshops.
- Experienced with user research strategy and execution to demonstrate user needs-based development.
- Experience of customer journey performance analysis and evaluation demonstrating understanding of user behaviour and highlighting future improvement opportunities.
- Experienced with business analysis including problem framing, business process modelling and improvement, value/benefits definition, scope definition, user story definition and management, stakeholder management and facilitation, success criteria definition.

36.8 **Accessibility**

- The Authority is committed to delivering public services that are accessible to all. This includes complying with the Public Sector Bodies Accessibility Regulations (PSBAR) 2018 by ensuring our services meet the Web Content Accessibility Guidelines (WCAG) 2.1. All services must meet this standard to a minimum of AA level or have a clear and timebound road map towards meeting the standard. This commitment is embodied in the accessibility statements that each service publishes. Compliance with the regulations and the standard is monitored and enforced by the CDDO.
- Experience of using these standards to deliver public facing digital services.

36.9 **CDDO Design Principles**

- Experience of using CDDO Design Principles and Digital Service Standard to deliver public facing digital services, outlining the principles applied, methods adopted and ability to deliver successful outcomes.
- CDDO Design Principles information can be found at:

  https://www.gov.uk/guidance/government-design-principles
- CDDO Service Standard information can be found at:

  https://www.gov.uk/service-manual/service-standard

36.10 **Content Design**

- Experience of using CDDO content design standards. Information about CDDO content design standards is at:

  https://www.gov.uk/guidance/content-design

36.11 **Knowledge Transfer**

- Experience of good practices around documentation/knowledge transfer as standard ways of working. Examples Include:
- Business process diagrams
- Technical information
- Annotated code
- User research outputs
- Customer journey maps
- Service blueprints
- Prototypes
- Experience with CDDO audit and assessment
- Experience coaching partners and teams with Agile practices

36.12 **IMS**

- Experience in understanding and defining system security requirements.
- Experience of preparing and documenting standard operating procedures and protocols.
- Configure and troubleshoot security infrastructure devices.
- Develop technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
- Facilitate in the detection and remediation of security incidents.
- Write comprehensive reports, including assessment-based findings, outcomes and propositions for further system security enhancement.
- All staff must be entitled to the appropriate security clearance as outlined in Section 35.19

36.13 **Data Protection**

- Experience of ensuring staff involved in data processing receive appropriate guidance and training.

- Experience of conducting compliance audits as required to ensure compliance and address potential issues proactively.
- Experience of serving as the point of contact between CI teams and IMS Data Team
- Experience of monitoring compliance and provide advice on the impact of new uses of data within projects/services and involving third parties.

36.14 **Further Requirements**

The supplier must be able to demonstrate a culture of continuous improvement.

37 Performance Management

37.1 Performance for the contract will be managed by regular reviews against work in progress as specified in Statements of Work (SoW). Reviews of progress will include:

- Tracking progress against roadmaps
- Use of a timeboxed approach to delivery – to demonstrate completion to plan.
- User story mapping
- Epics/sizing
- Sprint reviews – reporting/backlogs/burndown charts (to show completion, velocity, continuous improvement of team performance) with specific attention on variance what was planned versus what was delivered
- Service Management Boards
- Services for the candidate portal are delivered in line with CDDO and Authority standards (coding standards for example). Trainer Booker portal, IHTTC portal, incident management portal are not public facing.
- Analysis of first month critical bugs identified in production against the SoW.
- Balanced scorecard and monthly review of performance against KPI's as listed in document Annexe A – KPI's.

37.2 Work to be delivered by the supplier as part of this contract will be specified in a specific SoW to be agreed between the Authority and the Supplier.

37.3 Each SoW will include:

- Specific measurable deliverables, including metrics;
- Timescales for delivery;
- Supplier cost of delivery;
- Risks, assumptions and dependencies

APPENDIX C – FURTHER COMPETITION QUESTIONNAIRE

38 Introduction

38.1 Appendix C sets out the questions that will be evaluated as part of this Further Competition.

38.2 The following information has been provided in relation to each question (where applicable):

- Weighting – highlights the relative importance of the question;
- Guidance – sets out information for the Potential Provider to consider when preparing a response; and
- Marking Scheme – details the marks available to evaluators during evaluation.

39 Document Completion

39.1 Potential Providers must provide an answer to every question within the Jaggaer e-sourcing system. **This form is for information only and must not be used to submit your answers.**

39.2 Potential Providers must not alter / amend the document in any way.

39.3 Potential Providers must not submit any additional information with your Tender other than that specifically requested in this document.

40 Pass/Fail Questions

Please Note: The following questions are Pass / Fail questions, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer in the Jaggaer e-sourcing system.

Pass/Fail Questions			Pass/Fail
Please Note: The following question[s] is a [Pass / Fail] question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
[3.1]	Do you have the capacity to provide the full range of essential Software Development skills as detailed in section 36.2 of the specification	Yes	No
[3.2]	Do you have the capacity to provide the full range of essential Software Testing skills as detailed in section 36.3 of the specification?	Yes	No

[3.3]	Do you have the capacity to provide the full range of essential Architecture skills as detailed in section 36.4 of the specification?	Yes	No
[3.5]	Do you have the capacity to provide the full range of essential Data skills as detailed in section 36.5 of the specification?	Yes	No
[3.6}	Do you have the capacity to provide the full range of essential Delivery Management skills as detailed in section 36.6 of the specification?	Yes	No
[3.7]	Do you have the capacity to provide the full range of essential Service Design skills/experience as detailed in section 36.7 of the specification?	Yes	No
[3.8]	Do you have the capacity to provide the full range of essential Accessibility skills/experience as detailed in section 36.8 of the specification?	Yes	No
[3.9]	Do you have the capacity to provide the full range of essential skills/experience of CDDO Design Principles as detailed in section 36.9 of the specification?	Yes	No
[3.10]	Do you have the capacity to provide the full range of essential skills/experience of Content Design as detailed in section 36.10 of the specification?	Yes	No
[3.11]	Do you have the capacity to provide the full range of essential skills/experience of Knowledge transfer as detailed in section 36.11 of the specification?	Yes	No
[3.12]	Do you have the capacity to provide the full range of essential skills/experience of IMS as detailed in section 36.12 of the specification?	Yes	No
[3.13]	Do you have the capacity to provide the full range of essential skills/experience of Data Protection as detailed in section 36.13 of the specification?	Yes	No
[3.14}	Do you or your sub-contractor (where appropriate) hold certified Microsoft Cloud partner status?	Yes	No

41 Technical Evaluation

Question 1	Weighting 12%
Guidance:	
When describing the engagement context could you please include details of: • Size • Type of engagement (consultative, delivery partner, consortium bid) • Scope/Complexity • Whether it was an existing or new system • Architecture patterns adopted throughout the project or service lifecycle • Tools (Tech Stack) used to perform the project or service	

- Initial level of experience with the technology
- Approach to client engagement
- Any other relevant situational context

A good response should include evidence of the following points:

- What was the approach
- What documentation was completed
- Was it up to date
- How was it made available to client organisation
- Timescale to transfer
- Did the supplier take this approach from the beginning of their work (recognising theneed for knowledge transfer early and not waiting until close to the end of the contract)
- Platform or document management system used for the knowledge transfer
- Has delivered Continuous Improvement pipelines/backlogs
- Has demonstrated business process improvements; operational efficiency/financial efficiency or savings
- Skills transfer – experience in transferring skills to client/new supplier
- Process change – experience in highlighting changes to business processes during deliverables made during a project or service.
- Experience of knowledge transfer at handover of completed work package
- Experience of knowledge transfer on handover at end of contract

Question 1:	
Please give a specific example of when you have taken on an existing product and subsequently transferred knowledge to a client organisation or supplier, both during the project or contract, and at the end of a project or contract. How did you engage with stakeholders, in order to ensure the objectives of knowledge transfer were achieved.	
Maximum [500] words	
Marking Scheme:	
The following marking scheme will be used to assess the response provided to this question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high

	level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 2	Weighting 12%
Guidance:	
When describing the engagement context could you please include details of: • Size • Type of engagement (consultative, delivery partner, consortium bid) • Scope/Complexity • Whether it was an existing or new system • Architecture patterns adopted throughout the project or service lifecycle • Tools (Tech Stack) used to perform the project or service • Initial level of experience with the technology • Approach to client engagement • Any other relevant situational context A good response should include evidence of the following points: • Monitoring of code quality • Addressing security concerns • Prioritisation of issues • Use of technical backlog or tech debt register for making them visible and trackable. • Comparable scaled system development and delivery using the platform, infrastructure tools, runtimes and languages described • Proven technical competency in the roles listed and ability to provide and scale this expertise as required • Proven technical experience in using the core technologies described	
Question 2:	
Provide an example of an engagement whereby you were engaged for a substantial period of time maintaining and improving the same product or suites of products. What measures did you introduce to identify and manage inherited technical debt, how did you ensure a quality product was delivered to the customer, what was the approach you took to keep the system current and explain measures you put in place to guide you?	
Maximum [500] words	
Marking Scheme:	
The following marking scheme will be used to assess the response provided to this question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of

	confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 3	Weighting 12%
Guidance:	
When describing the engagement context could you please include details of: • Size • Type of engagement (consultative, delivery partner, consortium bid) • Scope/Complexity • Whether it was an existing or new system • Architecture patterns adopted throughout the project or service lifecycle • Tools (Tech Stack) used to perform the project or service • Initial level of experience with the technology • Approach to client engagement • Any other relevant situational context A good response should include evidence of the following points: • Clear examples and understanding of TDD • Test plans • Metrics for test coverage and improvements • Descriptions of testing activities • Understanding of test pyramid • Technique and approach used for automation to ensure it is maintainable and scalable. • Clear example of the use and understanding of continuous integration. • Approach to dealing with negative situations. • Comparable scaled system development and delivery using the platform, infrastructure tools, runtimes and languages described • Proven technical competency in the roles listed and ability to provide and scale this expertise as required • Proven technical experience in using the core technologies described	
Question 3:	
Provide an example of an engagement where you utilised automated testing/deployment, performance and load examination, continuous integration, technical documentation and delivered outcomes using TDD approaches. What were some negative situations you experienced during working on that project or service? How would you describe success for that project or service?	
Maximum [600] words	

Marking Scheme:	
The following marking scheme will be used to assess the response provided to this question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 4	Weighting 12%
Guidance:	

When describing the engagement context could you please include details of:

- Size (of engagement, userbase and volumes)
- Type of engagement (consultative, delivery partner, consortium bid)
- Scope/Complexity
- Whether it was an existing or new system
- Architecture patterns adopted throughout the project or service lifecycle
- Tools (Tech Stack) used to perform the project or service
- Initial level of experience with the technology
- Approach to client engagement
- Any other relevant situational context

A good response should include evidence of the following points:

- Extensive use of Azure Components (e.g. Functions, Databricks, APIM), Power Platform / Dynamics 365 and related technologies (e.g. Power Apps (Portals / Model / Canvas), Power Automate, Power BI, Dataverse, Azure Synapse Data Link
- Extension of prebuilt Dynamic 365 solutions (e.g. Customer Engagement CRM) and associated Common Data Model to implement business specific requirements
- Application lifecycle management (ALM) with Microsoft Power Platform (inc. Portals, Flows)
- A B2C website/mobile (e.g. Javascript) WebAPI based integration to the Dataverse
- Code reviewing and pairing practices
- Agile working practices (TDD etc)
- Application of the Service Standards to Power App Portals

- CI/CD & IaC
- Knowledge sharing tactics
- Azure B2B patterns for working with trusted suppliers
- Comparable scaled system development and delivery using the platform, infra-structure tools, runtimes and languages described
- Proven technical competency in the roles listed and ability to provide and scale this expertise as required
- Proven technical experience in using the core technologies described

Question 4:

Provide an example of an engagement where you utilised the Microsoft Power Platform extending prebuilt Dynamics 365 Solutions and maintaining and improving independent Customer Web UIs. Describe how you integrated your teams into pre-existing technical teams and if appropriate, how these teams were augmented with external specialist partners.

Maximum [1000] words

Question 5	Weighting 12%

Guidance:

When describing the engagement context could you please include details of:

- Size
- Type of engagement (consultative, delivery partner, consortium bid)
- Scope/Complexity
- Whether it was an existing or new system
- Architecture patterns adopted throughout the project or service lifecycle
- Tools (Tech Stack) used to perform the project or service
- Initial level of experience with the technology
- Approach to client engagement
- Any other relevant situational context

A good response should include evidence of the following points:

- What standards were used (industry standard, client organisation standards, own organisation standards)
- What processes/practices were used for quality assurance/governance
- Used a repeatable process to maintain standards
- Evidence of processes to facilitate knowledge transfer
- Has delivered outcomes working in collaboration with client-based teams

Question 5:

How did you ensure consistent standards in previous engagement where you have had multiple teams on a project or service, and what did you do to contribute to maintaining quality and consistency of software product into production? How did you reduce risk to your customer without impacting future delivery?

Maximum [500] words

Marking Scheme:

The following marking scheme will be used to assess the response provided to this

question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 6	Weighting 12%
Guidance:	

A good response should include evidence of the following points:

- Sub-criteria for tackling inequality in the contract workforce
- Activities that demonstrate and describe the tenderer's existing or planned:
- Understanding of the issues affecting inequality in employment, skills and pay in the market, industry or sector relevant to the contract, and in the tenderer's own organisation and those of its key sub-contractors.
- Measures to tackle inequality in employment, skills and pay in the contract workforce. Illustrative examples:
- Inclusive and accessible recruitment practices, and retention-focussed activities.
- Offering a range of quality opportunities with routes of progression if appropriate, e.g. IT Level industry placements, students supported into higher level apprenticeships.
- Working conditions which promote an inclusive working environment and promote retention and progression.
- Demonstrating how working conditions promote an inclusive working environment and promote retention and progression.
- A time-bound action plan informed by monitoring to ensure employers have a workforce that proportionately reflects the diversity of the communities in which they operate, at every level.
- Including multiple women, or others with protected characteristics, in shortlists for recruitment and promotions.
- Using skill-based assessment tasks in recruitment.
- Using structured interviews for recruitment and promotions.
- Introducing transparency to promotion, pay and reward processes.
- Positive action schemes in place to address under-representation in certain pay grades.
- Jobs at all levels open to flexible working from day one for all workers.

- Collection and publication of retention rates, e.g. for pregnant women and new mothers, or for others with protected characteristics.
- Regular equal pay audits conducted.

Activities that demonstrate and describe the tenderer's existing or planned:

- Understanding of in-work progression issues affecting the market, industry or sector relevant to the contract, and in the tenderer's own organisation and those of its key sub-contractors.
- Inclusive and accessible development practices, including those provided in the Guide for line managers on recruiting, managing and developing people with a disability or health condition.
- Measures to support in-work progression to help people in the contract workforce, to move into higher paid work by developing new skills relevant to the contract.

Question 6:

Social Value - Please describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome (driving equal opportunity by tackling workforce inequality) and Award Criteria.

You should include:

- your 'Method Statement', stating how you will achieve this and how your commitment meets the Award Criteria, and
- a timed project plan and process, including how you will implement your commitment and by when. Also, how you will monitor, measure and report on your commitments/the impact of your proposals. You should include but not be limited to:
- timed action plan
- use of metrics
- tools/processes used to gather data
- reporting
- feedback and improvement
- transparency
- how you will influence staff, suppliers, customers and communities through the delivery of the contract to support the Policy Outcome, e.g. engagement, co-design/creation, training and education, partnering/collaborating, volunteering

Maximum [1000] words

Marking Scheme:

The following marking scheme will be used to assess the response provided to this question:

0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the

	Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 7	Weighting 12%
Guidance:	
When describing the engagement context could you please include details of: • Size • Type of engagement (consultative, delivery partner, consortium bid) • Scope/Complexity • What security standards were used • Technologies and techniques involved • Other non-technical security solutions utilised • Approach to client engagement • Key security challenges and issues • Any other relevant situational context A good response should include evidence of the following points: • General working practices • Knowledge sharing tactics • Comparable delivery of services and an understanding of how the security function overlays and integrates with other activities to ensure that the security assurance status is maintained • Proven security competency in the types of roles required and ability to provide and scale this expertise as required • Proven security experience in using the core technologies described • An understanding of key security issues and challenges with this type of service, how these can be identified and mitigated	
Question 7:	
Provide an example of an engagement where you have provided similar security-related CI services to the Theory Test Service including large volumes of personal data being processed, covering the range of security requirements (Outlined in Section 35), how you successfully managed and maintained the security posture of the service and how this would then be used to deliver the requirements in this Contract.	
Maximum [1000] words	
Marking Scheme:	
The following marking scheme will be used to assess the response provided to this question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder

	provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Question 8	Weighting 16%
Guidance:	
When describing the engagement context could you please include details of 1. Team size and anticipated roles 1. Management overhead 2. Proposed team structure including onshore / offshore split 3. Approach to client engagement 4. Key challenges and issues 5. Any other relevant situational context A good response should include evidence of the following points: 6. Organisational structure 7. General working practices 8. Lessons learnt based on similar engagements 9. How the proposed team will deliver maximum value and benefit within the contract value	
Question 8:	
Detail how the Service Provider's delivery team will interact with the internal DVSA team to successfully deliver multiple streams of work in parallel. Your response should include: • The resource that the Service Provider intends to deploy and the proposed organisation structure • Proposed split between onshore and offshore resources • Your approach to managing successful/compliant delivery of work and overall performance • How you will ensure availability of the Service Provider's delivery team within the core hours of GMT • How the proposed team will deliver maximum value and benefit within the contract value	
Maximum [1000] words	

Marking Scheme:	
The following marking scheme will be used to assess the response provided to this question:	
0	Unanswered or totally inadequate response - Limited or no evidence is provided that leads to the conclusion that the bidder can meet very few of the requirements, giving no confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting less than 30% of the criteria as listed in the guidance.
1	Minimal/partial Response - Some evidence is provided that leads to the conclusion that the bidder can meet few of the requirements, giving a low level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 30% - 60% of the criteria as listed in the guidance.
2	Good Response - Evidence is provided that leads to the conclusion that the bidder can meet many of the requirements, giving a medium level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting between 60% - 90% of the criteria as listed in the guidance.
3	Excellent Response - Comprehensive evidence is provided that leads to a conclusion that the bidder can meet most of the requirements, giving a very high level of confidence that the Bidder can deliver the required service. Bidder provides evidence of meeting 90% or more of the criteria as listed in the guidance.

Price

[5] PRICE	Weighting 25%
Guidance:	
Using the pricing templates provided in this ITT pack, please provide your SFIA rates as requested on the template and your transition costs. Based on the requirements as detailed in this document and the overall value of the contract please also provide details of any volume discount that will apply for years 3 and 4 in the box provided on the service price template. The score for price will be calculated based on the average rate and using the calculation explained below. All prices shall be in GBP and exclusive of VAT.	
Question:	
N/A	£
Marking Scheme:	
The maximum mark available for Price will be 25% (20% for service costs and 5% for transition costs). This mark will be awarded to the lowest priced Potential Provider. Remaining Potential Providers will receive a mark out of this maximum mark on a pro rata basis dependent on how far they deviate from the lowest price. The calculation that will be used to determine marks is as follows: Score = (Lowest Tender Price multiplied by 25) and then divided by Supplier Tender Price	

Crown Commercial Service

Driver &
Vehicle
Standards
Agency
(DVSA)

and

Kainos
Software Ltd

ETHICAL WALLS AGREEMENT

Crown Copyright 2021

Version history:

Document last reviewed by GLD on 1 March 2020

This Agreement is dated
Between

(1) Driver & Vehicle Standards Agency (the **"Buyer"**) [acting on behalf of the Crown] of 1 Unity Square, Queensbridge Road, Nottingham ; and

(2) Kainos Software Ltd, a company registered in Northern Ireland under registration number NI019370 whose registered office is at 4-6 Upper Crescent, Belfast, Northern Ireland, BT71NT

together the "**Parties**" and each a "**Party**".

BACKGROUND

A. The Buyer is obliged to ensure transparency, fairness, non-discrimination and equal treatment in relation to its procurement process pursuant to the Public Contracts Regulations 2015 (as amended) (the **PCR)**. The purpose of this document ("Agreement") is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Further Competition Procedure.

B. The Buyer is conducting a Further Procurement Procedure for the supply of Digital Outcomes and Specialists 5 Deliverables under a Call-Off Contract (the **"Purpose"**).

C. The Buyer has an obligation to deal with conflicts of interest as set out in Regulation 24 (1) of the PCR. The concept of conflict of interest is wide. In the PCR it is described as covering at least *"any situation where relevant staff members have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure"* (Regulation 24(2)). *"Staff members"* refers to staff members of the Buyer or of a procurement service provider acting on behalf of the Buyer who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure. *"Procurement service provider"* refers to a public or private body which offers ancillary purchasing activities on the market.

D. Pursuant to Regulation 41 of the PCR, the Buyer is under an obligation to ensure that competition is not distorted by the participation of any Framework Contract supplier acting as a bidder in a further competition procedure. Accordingly, the Buyer has identified that a potential distortion of competition could arise as a consequence of a bidder wishing to submit a Tender for this Further Competition Procedure, where it has also performed services for the Buyer under existing contractual arrangements or as a subcontractor under those same arrangements.

E. The Parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Supplier does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:

1 DEFINITIONS AND INTERPRETATION

1.1 The following words and expressions shall have the following meanings in this agreement and its recitals:

"**Affiliate**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"**Agreement**" means this ethical walls agreement duly executed by the Parties;

"**Bid Team**" means any Supplier, Affiliate, connected to the preparation of an FCP Response;

"**Central Government Body**" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:

a) Government Department;
b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
c) Non-Ministerial Department; or

d) Executive Agency.

"**Conflicted Personnel**" means any Supplier, Affiliate, staff or agents of the Supplier or an Affiliate who, because of the Supplier's relationship with the Buyer under any Contract have or have had access to information which creates or may create a conflict of interest;

"**Contract**" means the [contract for [ ] dated [ ] between the Buyer and the Supplier and/or an Affiliate;

"**Control**" means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and "**Controls**" and "**Controlled**" shall be interpreted accordingly;

"**Effective Date**" means the date of this Agreement as set out above;

"**Further Competition Procedure**" or "**FCP**" means an invitation to submit tenders issued by the Buyer as part of an FCP Process;

"**FCP Process"** means, with regard to the Purpose, the relevant procedure provided for in Framework Schedule 7 (Call-Off Award Procedure) of RM1043.7 Framework Contract which the Buyer has elected to use to select a contractor, together with all relevant information, correspondence and/or documents issued by the Buyer as part of that procurement exercise, all information, correspondence and/or documents issued by the bidders in response together with any resulting contract;

"FCP Response" means the tender submitted or to be submitted by the Supplier or an Affiliate [(or, where relevant, by an Other Bidder)] in response to an FCP;

"Other Affiliate" any person who is a subsidiary, subsidiary undertaking or holding company of any Other Bidder;

"Other Bidder" means any other bidder or potential bidder that is not the Supplier or any Affiliate that has or is taking part in the FCP Process;

"Parties" means the Buyer and the Supplier;

"**Professional Advisor**" means a supplier, subcontractor, advisor or consultant engaged by the Supplier under the auspices of compiling its FCP Response;

"**Purpose**" has the meaning given to it in recital B to this Agreement;

"**Representative"** refers to a person's officers, directors, employees, advisers and agents and, where the context admits, providers or potential providers of finance to the Supplier or any Affiliate in connection with the FCP Process and the representatives of such providers or potential providers of finance; and

"**Third Party**" means any person who is not a Party and includes Other Affiliates and Other Bidders.

1.2 Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.

1.3 Reference to the disclosure of information, or provision of access, by or to the Buyer or the Supplier includes disclosure, or provision of access, by or to the representatives of the Buyer or Representatives of the Supplier (as the case may be).

1.4 Reference to persons includes legal and natural persons.

1.5 Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.

1.6 Reference to clauses and recitals is to clauses of and recitals to this Agreement.

1.7 Reference to any gender includes any other.

1.8 Reference to writing includes email.

1.9 The terms "associate", "holding company", "subsidiary", "subsidiary undertaking" and "wholly owned subsidiary" have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words 'holds a majority of the voting rights' shall be changed to 'holds 30% or more of the voting rights', and other expressions shall be construed accordingly.

1.10 The words "include" and "including" are to be construed without limitation.

1.11 The singular includes the plural and vice versa.

1.12 The headings contained in this Agreement shall not affect its construction or interpretation.

2 ETHICAL WALLS

2.1 In consideration of the sum of £1 payable by the Buyer to the Supplier, receipt of which is hereby acknowledged, the Supplier:

2.1.1 shall take all appropriate steps to ensure that neither the Supplier nor its Affiliates and/or Representatives are in a position where, in the reasonable opinion of the Buyer, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier or its Affiliates or Representatives and the duties owed to the Buyer under the Contract or pursuant to an fair and transparent FCP Process;

2.1.2 acknowledges and agrees that a conflict of interest may arise in situations where the Supplier or an Affiliate intends to take part in the FCP Process and, because of the Supplier's relationship with the Buyer under any Contract, the Supplier, its Affiliates and/or Representatives have or have had access to information which could provide the Supplier and/or its Affiliates with an advantage and render unfair an otherwise genuine and fair competitive FCP Process; and

2.1.3 where there is or is likely to be a conflict of interest or the perception of a conflict of interest of any kind in relation to the FCP Process, shall comply with Clause 2.2.

2.2 The Supplier shall:

2.2.1 Not assign any of the Conflicted Personnel to the Bid Team at any time;

2.2.2 Provide to the Buyer a complete and up to date list of the Conflicted Personnel and the Bid Team and reissue such list upon any change to it;

2.2.3 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates results in information of any kind or in any format and however so stored:

(a) about the Contract, its performance, operation and all matters connected or ancillary to it becoming available to the Bid Team; and/or

(b) which would or could in the opinion of the Buyer confer an unfair advantage on the Supplier in relation to its participation in the FCP Process becoming available to the Bid Team;

2.2.4 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates and in particular the Bid Team results in information of any kind or in any format and however so stored about the FCP Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;

2.2.5 Ensure that confidentiality agreements which flow down the Supplier's obligations in this Agreement are entered into as necessary between the Buyer and the Supplier, its Affiliates, its staff, agents, any Conflicted Personnel, and between any other parties necessary in a form to be prescribed by the Buyer;

2.2.6 physically separate the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;

2.2.7 provide regular training to its staff, agents and its Affiliates to ensure it is complying with this Agreement;

2.2.8 monitor Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement ensure adherence to the ethical wall arrangements;

2.2.9 ensure that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and

2.2.10 comply with any other action as the Buyer, acting reasonably, may direct.

2.3 In addition to the obligations set out in Clause 2.1.1 and 2.1.3, the Supplier shall:

2.3.1 notify the Buyer immediately of all perceived, potential and/or actual conflicts of interest that arise;

2.3.2 submit in writing to the Buyer full details of the nature of the conflict including (without limitation) full details of the risk assessments undertaken, the impact or potential impact of the conflict, the measures and arrangements that have

been established and/or are due to be established to eliminate the conflict and the Supplier's plans to prevent future conflicts of interests from arising; and

2.3.3 seek the Buyer's approval thereto,

which the Buyer shall have the right to grant, grant conditionally or deny (if the Buyer denies its approval the Supplier shall repeat the process set out in clause 2.3 until such time as the Buyer grants approval or the Supplier withdraws from the FCP Process).

2.4 Any breach of Clause 2.1, Clause 2.2 or Clause 2.3 shall entitle the Buyer to exclude the Supplier or any Affiliate or Representative from the FCP Process, and the Buyer may, in addition to the right to exclude, take such other steps as it deems necessary where, in the reasonable opinion of the Buyer there has been a breach of Clause 2.1, Clause 2.2 or Clause 2.3.

2.5 The Supplier will provide, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.1 and 2.2 as reasonably requested by the Buyer.

2.6 The Buyer reserves the right to require the Supplier to demonstrate the measures put in place by the Supplier under Clauses 2.1.3 and 2.2.

2.7 The Supplier acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Buyer of the adequacy of such measures and does not discharge the Supplier of its obligations or liability under this Agreement.

2.8 The actions of the Buyer pursuant to Clause 2.4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Buyer.

2.9 In no event shall the Buyer be liable for any bid costs incurred by:

2.9.1 the Supplier or any Affiliate or Representative; or

2.9.2 any Other Bidder, Other Affiliate or Other Representative,

as a result of any breach by the Supplier, Affiliate or Representative of this Agreement, including, without limitation, where the Supplier or any Affiliate or Representative, or

any Other Bidder, Other Affiliate or Other Representative are excluded from the FCP Process.

2.10 The Supplier acknowledges and agrees that:

2.10.1 neither damages nor specific performance are adequate remedies in the event of its breach of the obligations in Clause 2; and

2.10.2 in the event of such breach by the Supplier of any of its obligations in Clause 2 which cannot be effectively remedied the Buyer shall have the right to terminate this Agreement and the Supplier's participation in the FCP Process.

3 SOLE RESPONSIBILITY

3.1 It is the sole responsibility of the Supplier to comply with the terms of this Agreement. No approval by the Buyer of any procedures, agreements or arrangements provided by the Supplier or any Affiliate or Representative to the Buyer shall discharge the Supplier's obligations.

4 WAIVER AND INVALIDITY

4.1 No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.

4.2 If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.

5 ASSIGNMENT AND NOVATION

5.1 Subject to Clause 5.2 the Parties shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Buyer.

5.2 The Buyer may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:

5.2.1 any Central Government Body; or

5.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and

5.2.3 the Supplier shall, at the Buyer's request, enter into a novation agreement in such form as the Buyer reasonably specify in order to enable the Buyer to exercise its rights pursuant to this Clause 5.

5.3 A change in the legal status of the Buyer such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Buyer.

6 CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

6.1 A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement but this does not affect any right remedy of any person which exists or is available otherwise than pursuant to that Act.

7 TRANSPARENCY

7.1 The Parties acknowledge and agree that the Buyer is under a legal duty pursuant to the PCR to run transparent and fair procurement processes. Accordingly, the Buyer may disclose the contents of this Agreement to potential bidders in the FCP Process, for the purposes of transparency and in order to evidence that a fair procurement process has been followed.

8 NOTICES

8.1 Any notices sent under this Agreement must be in writing.

8.2 The following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an email to the correct email address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next working day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

8.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

	Supplier	**Buyer**
Contact		

Address

Email		

8.4 This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

9 WAIVER AND CUMULATIVE REMEDIES

9.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended and what is waived. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

9.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

10 TERM

10.1 Each Party's obligations under this Agreement shall continue in full force and effect for a period of [ ] years from the Effective Date.

11 GOVERNING LAW AND JURISDICTION

11.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

11.2 The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

Signed by the Buyer Name:

Signature: Position

in Buyer:

Signed by the Supplier Name: Signature:

Position in Supplier: