Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	CR_4619
THE BUYER:	The Secretary of State for the Department of Business and Trade
BUYER ADDRESS	Old Admiralty Building, Westminster, London, SW1A 2BL
THE SUPPLIER:	Shakespeare Martineau LLP
SUPPLIER ADDRESS:	No 1 Colmore Square, Birmingham, B4 6AA
REGISTRATION NUMBER:	442480
DUNS NUMBER:	349812524
SID4GOV ID:	1341484

This Order Form, when completed and executed by both Parties, forms a Call-Off Contract. A Call-Off Contract can be completed and executed using an equivalent document or electronic purchase order system.

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 7 October 2024.

It's issued under the Framework Contract with the reference number RM6226 for the provision of Litigation Services.

CALL-OFF LOT:

Lot 6 - Litigation Services (England and Wales)

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. Joint Schedule 1 (Definitions and Interpretation) RM6226
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6226
        - Joint Schedule 2 (Variation Form and Change Control Procedure)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)
        - Joint Schedule 12 (Supply Chain Visibility)

    - Call-Off Schedules for RM6226
        - Call-Off Schedule 1 (Transparency Reports)
        - Call-Off Schedule 3 (Continuous Improvement)
        - Call-Off Schedule 5 (Pricing Details)
        - Call-Off Schedule 6 (ICT Services)
        - Call-Off Schedule 7 (Key Supplier Staff)
        - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
        - Call-Off Schedule 9 (Security Requirements)
        - Call-Off Schedule 10 (Exit Management)
        - Call-Off Schedule 13 (Implementation Plan and Testing)
        - Call-Off Schedule 14 (Service Levels)
        - Call-Off Schedule 15 (Call-Off Contract Management)
        - Call-Off Schedule 20 (Call-Off Specification)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility)

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:
None

CALL-OFF START DATE: 11 October 2024

CALL-OFF EXPIRY DATE: 31 March 2025

CALL-OFF INITIAL PERIOD: 6 Months

CALL-OFF OPTIONAL EXTENSION PERIOD A further period of up to 6 Months

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

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £500,000 (inc VAT)

CALL-OFF CHARGES
See details in Call-Off Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
All invoices should be sent, quoting a valid Purchase Order number (PO Number) in a PDF format, to the relevant authority at the addresses set out below including the following information:

- Invoice number
- Invoice date
- VAT registration number (where applicable)
- The Supplier's Company address and contact details
- The Supplier's bank details
- Description of Services provided

BUYER'S INVOICE ADDRESS:
Department for Business & Trade c/o UK SBS
Queensway House
West Precinct
Billingham
TS23 2NF

[redacted]

BUYER'S AUTHORISED REPRESENTATIVE

[redacted]
Commercial Lead – Corporate Services
[redacted]
Department of Business and Trade, UK Government Hub (Wales), Ty William Morgan, 6 Central Square, Wood Street, Cardiff, CF10 1EP

BUYER'S ENVIRONMENTAL POLICY
N/A

BUYER'S SECURITY POLICY
Government Functional Standard GovS 007: Security Version 1.0 – 24 July 2020 available online at:

https://www.gov.uk/government/publications/government-functional-standard-govs-007-security

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]
Partner
[redacted]
Shakespeare Martineau LLP, No 1 Colmore Square, Birmingham, B4 6AA

SUPPLIER'S CONTRACT MANAGER
[redacted]
Partner / Client Relationship Partner
[redacted]
Shakespeare Martineau LLP, No 1 Colmore Square, Birmingham, B4 6AA

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

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

BUYERS KEY STAFF
[redacted]
Assurance Manager
[redacted]
Department for Business and Trade, Citygate, Gallowgate, Newcastle upon Tyne, NE1 4JD

BUYERS KEY STAFF
[redacted]
Head of Employment Tribunals Financial Penalties Team
[redacted]
Department of Business and Trade, Second Floor, Rooms 2.14-2.15, Old Admiralty Building, London, SW1A 2DW

SUPPLIERS KEY STAFF
Name - [redacted]
Role - Client Relationship Manager
Email – [redacted]
Address - Bridgeway House, Bridgeway, Stratford upon Avon, CV37 6YX, DX 16202 Stratford Upon Avon.

Name - [redacted]
Role - Operations Manager
Email – [redacted]
Address - Bridgeway House, Bridgeway, Stratford upon Avon, CV37 6YX, DX 16202 Stratford Upon Avon.

Name – [redacted]
Role – Solicitor
Email – [redacted]
Address - No 1 Colmore Square, Birmingham, B4 6AA

Name – [redacted]
Role – Associate
Email – [redacted]
Address - No 1 Colmore Square, Birmingham, B4 6AA

Name - [redacted]
Training and Compliance Manager
Email – [redacted]
Address - Bridgeway House, Bridgeway, Stratford upon Avon, CV37 6YX, DX 16202 Stratford Upon Avon.

KEY SUBCONTRACTOR(S)
Key Subcontractor 1
Name (Registered name if registered): [redacted]
Registration number (if registered): [redacted]
Role of Subcontractor: ***Provision of High Court Enforcement services and tracing.***

Key Subcontractor 2
Name (Registered name if registered): [redacted]
Registration number (if registered): [redacted]
Role of Subcontractor: ***Provision of letter printing and postage services.***

Key Subcontractor 3
Name (Registered name if registered): [redacted]
Registration number (if registered): [redacted]
Role of Subcontractor: ***Provision of asset/property management services.***

Key Subcontractor 4
Name (Registered name if registered): [redacted]

Registration number (if registered): [redacted]
Role of Subcontractor: Provision of Advocacy services

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Service Credits will accrue in accordance with Call-Off Schedule 14 - Service Levels

The Service Period is: one Month.

Critical Service Level Failure: A Critical Service Level Failure will be deemed to have occurred if the number of Service Credits the Supplier accrues in any Service Period exceeds 500 Service Credits.

Service Levels are to be reviewed and revised as part of the future requirement of this call-off agreement.

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
There's a guarantee of the Supplier's performance provided for all Call-Off Contracts entered under the Framework Contract

SOCIAL VALUE COMMITMENT
Not applicable

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	Partner	Role:	Head of Commercial
Date:	7 October 2024	Date:	8 October 2024

Joint Schedule 2 (Variation Form and Change Control Procedure)

Part A - Variation Form

This Variation Form shall be used to make a Variation or Change (in accordance with the Change Control Procedure set out in Part B of this Schedule) to the Contract in accordance with Clause 24 (Changing the Contract).

Contract Details		
This variation is between:	**[delete** as applicable: Buyer(**"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]	
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		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Implementation Plan / Testing required;		
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: • **Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation Form must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

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

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

Signed by an authorised signatory for and on behalf of the Buyer

Signature	
Date	
Name (in Capitals)	
Address	

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

Signature	
Date	
Name (in Capitals)	
Address	

Part B Change Control Procedure

This Part B of this Schedule sets out the process to be followed when CCS or the Buyer wishes to make a Change in the way in which the Deliverables or Service is provided by the Supplier.

Definitions

The following definitions apply to this Schedule and are supplemental to those in Joint Schedule 1 (Definitions):

Actual Expenditure	the amount of money spent that a Supplier actually incurred in implementing a Change
Change	a change made to the way in which any Deliverables or Service is provided by the Supplier to the Buyer under the Call Off Contract, which has been requested by the Buyer and agreed with the Supplier as part of the Change Control Procedure;
Change Control Procedure	the processes and procedures to be followed by the CCS or Buyer (as appropriate) and Supplier in proposing, agreeing, executing, delivering, reporting and managing Changes to the Services or Deliverables under the Contract;
Change Implementation Plan	the plan provided by the Supplier to CCS or the Buyer (as appropriate) for the provision of the Deliverables set out in the draft Variation Form sent by the CCS or the Buyer to the Supplier and agreed by the Buyer or CCS (as applicable) in accordance with the Change Control Procedure;
Change Milestone Certificate	the Certificate issued by the Buyer when the Supplier has met all of the requirements of a Change Milestone set out in the Change Implementation Plan which implements the agreed the Change agreed in the Variation Form under the Change Control Procedure;
Change Milestone	an event or task described in the Change Implementation Plan;
Change Satisfaction Certificate	the certificate issued by CCS or the Buyer (as applicable) when the Supplier has met all of the requirements of a Change set out in the Change Implementation Plan in accordance with the Variation Form and the Change Control Procedure;
Change Test Success Criteria	in relation to any Test associated to a Change, the test success criteria for that Test;
Forecast Expenditure	the forecast money to be spent that a Supplier proposes to incur to implement a Change;

1. Variations and Change Management

- Any Variations that do not fall to be a Change shall (including any change to a Debt Type or introduction of a New Debt Type) be undertaken in accordance with Clause 24 (Changing the Contract) of the Core Terms.

- Where a Change is sought, the Parties shall comply with the Change Control Procedure set out in Part B of this Schedule as well as complying with Clause 24 of the Core Terms.

- Where a Change is an Operational Change, the Parties shall comply with Paragraph 6 of this Schedule.

- Any Variation or Change agreed under Paragraphs 1.1 and 1.2 above shall be recorded using the Variation Form in Part A of this Schedule.

Change Control Procedure

- **Approach to Change**

- This Schedule sets out a 2-tier Change Control Procedure which shall be used to ensure operational efficiency:

    2. Tier 1: Fast Track Change – to be used where the Buyer requires an immediate solution. The Buyer may request no more than 4 Fast Track Changes in any rolling 12-Month period.

    - Tier 2: Standard Change – to be used where CCS or the Buyer seeks a Change that is not a Fast Track Change.

- All CCS or Buyer requests for a Change must be delivered to the timelines set out in the executed Variation Form, unless otherwise agreed in writing between the relevant Parties. CCS or the Buyer, acting reasonably, will establish the timelines by which any Change shall be delivered by the Supplier. CCS or the Buyer, at their sole discretion may accept an alteration to the timescales in writing.

- **Tier 1: Fast Track Change:** Upon receipt of the Buyer's request for a Change, the Supplier shall provide an Impact Assessment for the proposed Change within 5 Working Days of the date of the Buyer's request. The request shall be in the form of a draft Variation Form. The Buyer shall indicate in the draft Variation Form whether it is seeking to use the Tier 1: Fast Track Change or Tier 2: Standard Change procedure.

- The Buyer and the Supplier may agree in writing to vary Tier 1: Fast Track Change parameters from time to time.

- The Buyer shall be able to make a Tier 1: Fast Track Change request at any time after the satisfactory completion and acceptance of all Change Milestones and Tests regarding the Change Implementation Plan in accordance with Call-Off Schedule 13 (Implementation Plan and Testing).

Any Change requests that fall within the Change Implementation Plan period will not amount to a Tier 1: Fast Track Change or Tier 2: Standard Change.

- **Tier 2: Standard Change:** Upon receipt of a Buyer's Change request, the Supplier shall provide an Impact Assessment for the proposed Change within 20 Working Days of the date of issue on the draft Variation Form from CCS or the Buyer (as appropriate), unless otherwise specified in writing by the Buyer in the draft Variation Form.

- If the Supplier has any questions regarding the content of the draft Variation Form submitted by CCS or the Buyer, the Supplier must clarify these with CCS or the Buyer before the Supplier provides the Impact Assessment to CCS or the Buyer within the 5 Working Days for Tier 1: Fast Track Changes, or 20 Working Days for a Tier 2: Standard Change, unless otherwise agreed in writing between the Supplier and CCS or the Buyer (as applicable).

- The Supplier must use their expertise and innovation to provide a solution for delivering the Changes required by CCS or the Buyer within the applicable timeframes and ensuring that CCS or the Buyer's requirements are met.

- Where CCS or the Buyer requires further clarification or amendment to be made to the Impact Assessment to ensure CCS or the Buyer (as applicable) accept the Impact Assessment, the Supplier must return their response to the further clarification or amendment regarding the Change request within 2 Working Days of receipt for a Tier 1: Fast Track Change or within 5 Working Days of receipt for a Tier 2: Standard Change.

- The Supplier shall monitor and manage all aspects of Change delivery and maintain dialogue with CCS or the Buyer (as appropriate), as to the status of the Change. If the Supplier expects any delays to its delivery the Supplier shall inform CCS or the Buyer (as applicable) of the reason for the delay, why it has or may occur and how long it will take to resolve.

- The Supplier shall work with Subcontractors to ensure that appropriate Change deliverables and timelines are agreed, fully understood and implemented in accordance with the agreed Change as set out in the agreed Variation Form.

- In the case of either a Tier 1: Fast Track Change or a Tier 2: Standard Change, the Supplier shall provide the Buyer with any additional information requested on an Open Book Data basis, including breakdowns of all costs associated with the proposed Change.

- Any Charges Approved by the Buyer associated with delivering the Change shall be calculated using **table 4 at Annex 1 of Framework Schedule 3 (Framework Prices).**

● Implementing a Change

- Where a Change requires an Implementation Plan, the Variation Form shall include a draft Change Implementation Plan produced by the Supplier detailing at least, as a minimum, one Milestone marking the delivery of the applicable Change.

- The Buyer will issue a Change Milestone Certificate when the Buyer has confirmed that they are satisfied that the relevant Change Milestone has been Achieved.

- The Buyer will only accept the Change as being delivered once it has Approved the final Change Milestone of the Change Implementation Plan.

- The Supplier must monitor its performance against the Change Implementation Plan and the agreed Change Milestones and report its progress to the Buyer.

- The Supplier shall work with all Subcontractors to ensure that appropriate Change Deliverables and timelines are agreed, fully understood and implemented as set out in the agreed Variation Form.

- Where there is a cost Approved for the delivery of a Change, the invoice for that Change can only be submitted for payment by the Supplier, either:
  - once CCS or the Buyer has Approved the Change as having been completed satisfactorily and after the final Change Milestone Certificate has been issued; or
  - in accordance with the Change Milestones agreed by CCS or the Buyer within the Impact Assessment.

● Change Testing

- Where CCS or the Buyer requires Testing as part of Change implementation, the Buyer and Supplier shall comply with Call-Off Schedule 13 (Implementation and Testing) Part B (Testing) when developing the Change Implementation Plan. The Buyer shall agree with the Supplier what and how the Call-Off Schedule 13 Part B (Testing) shall apply relative to the scope and impact of the Change and include this as part of any Change Milestone Criteria.

● Change Delivery Reporting

- The Supplier shall report upon the progress of all Variations and Changes made Monthly and this must include as a minimum:

  3. Performance against Service Levels;
  4. Any risks, issues and mitigations impacting the Change Implementation Plan and Change Milestones; and
  5. Forecast Expenditure on the Change versus Actual Expenditure on the Change and updated forecast total costs of the Change

  Progress shall be reported to:

  - CCS as part of the Supplier's MI and reporting obligations set out in Framework Schedule 5 (Management Charges and Information); and
  - The Buyer as part of the Supplier's obligations to comply with Call-Off Schedule 1 (Transparency Reporting).

● Changes permissible outside of the Change Control Procedure

- Where the Buyer requires an Operational Change to an existing operational process or procedure performed by either the Supplier or its Subcontractor, for example,' where Buyer internal policy &/or guidance is updated, resulting in the need to reflect that update in the Supplier guidance, this will not be a Change that requires the Parties to comply with the Change Control Procedure nor to follow the Variation Procedure unless the Operational Change incurs additional cost or materially impact on the Supplier's resources, in which case the Buyer shall comply with the Change Control Procedure.

- Where the Buyer requires an Operational Change to be made, it shall submit a written request disclosing details of the proposed request for Operational Change and the proposed timescales for its completion.

- The Supplier shall prepare a solution for consideration by and Approval of the Buyer, prior to implementation of it by a date agreed.

- The Supplier shall not implement any Operational Change without the Approval of the Buyer.

Joint Schedule 3 (Insurance Requirements)

1. **The insurance you need to have**

   - 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:
     - the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
     - the Call-Off Contract Effective Date in respect of the Additional Insurances.
   - The Insurances shall be:
     - maintained in accordance with Good Industry Practice;
     - (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;
     - taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
     - maintained for at least six (6) years after the End Date.
   - 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.

- **How to manage the insurance**

   - Without limiting the other provisions of this Contract, the Supplier shall:
     - 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;
     - promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
     - 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.

- **What happens if you aren't insured**

  - 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.
  - 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.

- **Evidence of insurance you must provide**

  - 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.

- **Making sure you are insured to the required amount**

  - 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.

- **Cancelled Insurance**

  - 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.
  - 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.

- **Insurance claims**

  - 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.

- 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.
- Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 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 their first Call Off Contract Start Date in accordance with this Schedule:

   i. **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) – applicable to all 20 Lots; and

   ii. **public liability insurance, professional indemnity insurance, comprehensive crime insurance and cyber insurance** with cover (for a single event or a series of related events and in the aggregate) of, amongst other, amounts not less than those specified in the table below on a per Lot basis:

Lot No.	Service	Public Liability	Professional Indemnity	Comprehensive Crime	Cyber Insurance
1	Collections	£5m	£5m	£5m	£5m
2	a) Data Reports b) Monitoring and Alerts c) Products	£1m	£1m	£1m	n/a
3	Affordability Assessment and Monitoring	£1m	£1m	£1m	n/a
4	FED Advisory	£1m	£1m	£1m	n/a
5	Enforcement	£5m	£5m	£5m	£5m
6	Litigation England and Wales	£2m	£2m	£2m	£2m
7	Litigation Scotland	£2m	£2m	£2m	£2m
8	UK Auctioneers Services London	£1m	£1m	£1m	n/a
9	UK Auctioneers Services South	£1m	£1m	£1m	n/a
10	UK Auctioneers Services Midlands	£1m	£1m	£1m	n/a
11	UK Auctioneers Services North	£1m	£1m	£1m	n/a
12	UK Auctioneers Services Wales	£1m	£1m	£1m	n/a
13	UK Auctioneers Services Northern Ireland	£1m	£1m	£1m	n/a
14	Process Servers	£1m	£1m	£1m	n/a
15	Spend Analytics and Recovery Services (SARS) AP Review	£1m	£1m	£1m	n/a
16	SARS General Compliance Review	£1m	£1m	£1m	n/a
17	SARS Specialist Review Utilities	£1m	£1m	£1m	n/a
18	SARS Specialist Review Utilities	£1m	£1m	£1m	n/a
19	SARS Specialist Review VAT	£1m	£1m	£1m	n/a
20	Managed Enforcement	£5m	£5m	£5m	£5m

Joint Schedule 4 (Commercially Sensitive Information)

1. **What is the Commercially Sensitive Information?**

i. 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.

ii. 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).

iii. 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:

Date, Item(s) and Duration of Confidentiality
Date: 18.08.2021 Details: (1) Commercial response: Attachment 3 Price Matrix. (2) Commercial Response: Attachment 3.1 Price Scenarios. (3) Section H: Litigation processes. (4) Section H2: Client Service and value for money. (5) Contract example certificate. Duration of confidentiality: Duration of the framework.

Joint Schedule 6 (Key Subcontractors)

1. **Restrictions on certain subcontractors**

i. The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

ii. The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

iii. 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 CCS and the Buyer **(with whom it has entered into a Call Off Agreement and/ or Lease Agreement)** and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

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

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

  iii. the proposed Key Subcontractor employs unfit persons.

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

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

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

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

  iv. for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;

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

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

v. If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:

i. a copy of the proposed Key Sub-Contract; and

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

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

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

ii. 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;

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

iv. 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;

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

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

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

3. the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

4. 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

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

vi. 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 (What happens if the contract ends) of this Contract; and

vii. 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**

o 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: i. the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; ii. 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; iii. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; iv. Monitored Company committing a material breach of covenant to its lenders; v. 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 vi. 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.

- **When this Schedule applies**
  - 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.
  - The terms of this Schedule shall survive:
    - 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
    - under the Call-Off Contract until the termination or expiry of the Call-Off Contract.
- **What happens when your credit rating changes**
  - 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.
  - 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.

- 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 written calculations of

  the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

$$\frac{A+B+C}{D}$$

  where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company].

- The Supplier shall:
  - regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and
  - promptly notify (or shall procure that its auditors promptly notify) CCS 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.
- 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.

- **What happens if there is a financial distress event**

  - 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.
  - [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:
    - rectify such late or non-payment; or
    - demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.]
  - The Supplier shall and shall procure that the other Monitored Companies shall:
    - 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
    - where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) 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:
      - 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
      - provide such financial information relating to the Monitored Company as CCS may reasonably require.
  - 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.
  - 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.

- Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:
    - 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;
    - 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
    - comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).
- 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 4.64.6.
- 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.

- **When CCS or the Buyer can terminate for financial distress**

    - CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:
        - the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;
        - 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; and/or
        - 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.

- If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

- **What happens If your credit rating is still good**

  - 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:

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

[Rating Agency 1]

[Rating Agency 2]

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	**Credit rating (long term)**
Supplier	[D&B Threshold]

Joint Schedule 10 (Rectification Plan)

Request for Rectification Plan			
Details of the Default:	Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by Buyer :		Date:	
Supplier Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
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	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Definitions

. 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

. 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:

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

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

() "Joint Controller" with the other Party;

() "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

. 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.

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

. 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 systematic description of the envisaged Processing and the purpose of the Processing;

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

() an assessment of the risks to the rights and freedoms of Data Subjects; and

() the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

() 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;

() 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:

() nature of the data to be protected;

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

() state of technological development; and

() cost of implementing any measures;

() ensure that :

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

() 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:

() 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;

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

() 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

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

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

() 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;

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

() 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

() 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

() 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.

. 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:

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

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

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

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

() 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

() becomes aware of a Personal Data Breach.

. 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.

. 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:

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

() 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;

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

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

() 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.

. 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:

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

() 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

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

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

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

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

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

() obtain the written consent of the Controller;

() 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

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

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

. 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).

. 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

. 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

. 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.

. 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.

. 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.

. 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.

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

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

() 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

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

. 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.

. 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.

. 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")**:

() 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

() 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:

() 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

() 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.

. 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:

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

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

() 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

() 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.

. 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).*

. 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)*.

. 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.

. The contact details of the Relevant Authority's Data Protection Officer are: [redacted]
. The contact details of the Supplier's Data Protection Officer are: [redacted].
. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
. Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**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:* *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. of information relating to the Business contact details of any directors, officers, employees, agents, consultants and contractors of the Relevant Authority and the Supplier* *for the purposes of managing the relationship between the Parties:*
Duration of the Processing	*The term of the Contract plus 6 years, unless specified otherwise in that Party's privacy notice and/or retention schedule, as notified to the other parties in writing.*
Nature and purposes of the Processing	*The Processing of Personal Data is for the purposes of managing the contractual relationship between the Parties and to evidence compliance with legal, professional and/or regulatory obligations on each Party, and is undertaken on the following purposes, as set out in Article 6 of the GDPR, including* *a) Where the Processing is necessary for:*

	a. Compliance with a legal obligation to which that Party is subject; *b. The performance of a task carried out int eh public interest or in the exercise of official authority vested in that Party;* *c. The purposes of the legitimate interests pursued by that or any other third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child (and in respect of the Relevant Authority, where no other grounds set out above are applicable); or* *b) Where the data subject has consented to the Processing of their personal data for one or more specified purposes.*
Type of Personal Data	• *Name* • *Job title* • *Business Address;* • *Workplace telephone number;* • *E-mail address;* • *Authority* • *Any other personal data volunteered by the Data Subject*
Categories of Data Subject	*Employees of the Relevant Authority, Suppliers and/or Sub-Contractors (including contractors and employees of any contractors appointed by any of the Parties)*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to	*Personal Data will be retained in accordance with each Party's retention schedule or privacy notice, unless required by law or retain this information for longer, and then securely and irretrievably deleted.*

preserve that type of data	

Joint Schedule 12 (Supply Chain Visibility)

. **Definitions**

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

"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"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 sized enterprises;
"Supply Chain Information Report Template"	the document at Annex 1 of this Schedule 12; and
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

- **Visibility of Sub-Contract Opportunities in the Supply Chain**

  - The Supplier shall:

    - subject to Paragraph 2.3, advertise on Contracts Finder all Sub-Contract opportunities arising from or in connection with the provision of the Deliverables above a minimum threshold of £25,000 that arise during the Contract Period;
    - within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;
    - monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;
    - provide reports on the information at Paragraph 2.1.3 to the Relevant Authority in the format and frequency as reasonably specified by the Relevant Authority; and

- promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

- Each advert referred to at Paragraph 2.1.1 of this Schedule 12 shall provide a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

- The obligation on the Supplier set out at Paragraph 2.1 shall only apply in respect of Sub-Contract opportunities arising after the Effective Date.

- Notwithstanding Paragraph 2.1, the Authority may by giving its prior Approval, agree that a Sub-Contract opportunity is not required to be advertised by the Supplier on Contracts Finder.

- **Visibility of Supply Chain Spend**

- In addition to any other management information requirements set out in the Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME management information reports (the "SME Management Information Reports") to the Relevant Authority which incorporates the data described in the Supply Chain Information Report Template which is:

1. the total contract revenue received directly on the Contract;
2. the total value of sub-contracted revenues under the Contract (including revenues for non-SMEs/non-VCSEs); and
3. the total value of sub-contracted revenues to SMEs and VCSEs.

- The SME Management Information Reports shall be provided by the Supplier in the correct format as required by the Supply Chain Information Report Template and any guidance issued by the Relevant Authority from time to time. The Supplier agrees that it shall use the Supply Chain Information Report Template to provide the information detailed at Paragraph 3.1(a) –(c) and acknowledges that the template may be changed from time to time (including the data required and/or format) by the Relevant Authority issuing a replacement version. The Relevant Authority agrees to give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used.

- The Supplier further agrees and acknowledges that it may not make any amendment to the Supply Chain Information Report Template without the prior Approval of the Authority.

Annex 1

Supply Chain Information Report template

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
[Performance]	[ ]	[ ]	[ ]
[Call-Off Contract Charges]	[ ]	[ ]	[ ]
[Key Subcontractors]	[ ]	[ ]	[ ]
[Technical]	[ ]	[ ]	[ ]
[Performance management]	[ ]	[ ]	[ ]

Call-Off Schedule 3 (Continuous Improvement)

1. **Buyer's Rights**

i. 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**

i. 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.

ii. 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.

iii. 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:

   i. identifying the emergence of relevant new and evolving technologies;

   ii. 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);

   iii. 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

   iv. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

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

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

  ii. 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.

ix. 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.

x. 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.

xi. 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.

xii. 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 5 (Pricing Details)

Charges for services delivered under Lot 6 of RM6226 will be in accordance to the Rate Card below:

Call-Off Schedule 6 (ICT Services)

1. **Definitions**

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

"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;
"Defect"	any of the following: o any error, damage or defect in the manufacturing of a Deliverable; or o any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or
	o 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 o 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;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Subcontractors 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;
"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: o the Deliverables are (or are to be) provided; or o the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or o 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 (i) from, to or at which physical interface with the Buyer System takes place or (ii) where any part of the Supplier System is situated;

"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 Subcontractor 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;

- **When this Schedule should be used**
    - This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.
- **Buyer due diligence requirements**
    - The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
        - suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
        - operating processes and procedures and the working methods of the Buyer;
        - ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
        - 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.

- The Supplier confirms that it has advised the Buyer in writing of:
  - each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
  - the actions needed to remedy each such unsuitable aspect; and
  - a timetable for and the costs of those actions.

- **Licensed software warranty**
  - The Supplier represents and warrants that:
    - it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Subcontractor) 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;
    - all components of the Specially Written Software shall:
      - be free from material design and programming errors;
      - perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
      - not infringe any IPR.

- **Provision of ICT Services**
  - The Supplier shall:
    - 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;
    - 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;
    - ensure that the Supplier System will be free of all encumbrances;

- ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
- minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

- **Standards and Quality Requirements**
  - 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**")**.**
  - 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.
  - Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
  - The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
    - be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
    - 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
    - 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.

- **ICT Audit**
  - The Supplier shall allow any auditor access to the Supplier premises to:
    - inspect the ICT Environment and the wider service delivery environment (or any part of them);
    - review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
    - review the Supplier's quality management systems including all relevant Quality Plans.

- **Maintenance of the ICT Environment**
    - 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.
    - 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.
    - The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
    - 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.

- **Intellectual Property Rights in ICT**
    - **Assignments granted by the Supplier: Specially Written Software**
        - 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:
            - the Documentation, Source Code and the Object Code of the Specially Written Software; and
            - 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**").
        - The Supplier shall:
            - inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
            - 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

- 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.

- 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.

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

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

1. of its own Existing IPR that is not COTS Software;

2. third party software that is not COTS Software

  - Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants 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.

- 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:
    - 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
    - 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.
- 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.
- 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.

o **Licenses for COTS Software by the Supplier and third parties to the Buyer**

- 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.
- 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.
- 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.
- 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:

- will no longer be maintained or supported by the developer; or
- will no longer be made commercially available

- **Buyer's right to assign/novate licences**
  - The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 9.2 (to:
    - a Central Government Body; or
    - 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.
  - 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.
- **Licence granted by the Buyer**
  - 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).
- **Open Source Publication**
  - 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:
    - suitable for publication by the Buyer as Open Source; and
    - based on Open Standards (where applicable),

    and the Buyer may, at its sole discretion, publish the same as Open Source.
  - The Supplier hereby warrants that the Specially Written Software and the New IPR:
    - 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;

- 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;
- do not contain any material which would bring the Buyer into disrepute;
- can be published as Open Source without breaching the rights of any third party;
- 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
- do not contain any Malicious Software.

▪ 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:

- 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
- 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.

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.

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; and

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.

1.6 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

i. 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"	● has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	● 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"	● the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	● has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	● the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	● any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;

"Review Report"	● has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	● has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

i. 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.

ii. Within 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:

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

  ii. the recovery of the Deliverables in the event of a Disaster

iii. The BCDR Plan shall be divided into three sections:

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

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

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

iv. 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)

i. Section 1 of the BCDR Plan shall:

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

  ii. 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;

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

iv. 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;

v. 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;

vi. contain a risk analysis, including:

1. failure or disruption scenarios and assessments of likely frequency of occurrence;

2. identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

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

4. a business impact analysis of different anticipated failures or disruptions;

vii. provide for documentation of processes, including business processes, and procedures;

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

ix. identify the procedures for reverting to "normal service";

x. 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;

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

xii. 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.

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

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

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

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

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

iii. 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.

iv. 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)

i. 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:

i. 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

ii. 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.

ii. The Business Continuity Plan shall:

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

ii. 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;

iii. 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

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

5. Disaster Recovery (Section 3)

i. 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.

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

i. loss of access to the Buyer Premises;

ii. loss of utilities to the Buyer Premises;

iii. loss of the Supplier's helpdesk or CAFM system;

iv. loss of a Subcontractor;

v. emergency notification and escalation process;

vi. contact lists;

vii. staff training and awareness;

viii. BCDR Plan testing;

ix. post implementation review process;

x. 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;

xi. 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;

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

xiii. testing and management arrangements.

6. Review and changing the BCDR Plan

i. The Supplier shall review the BCDR Plan:

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

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

iii. 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.

ii. 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.

iii. 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.

iv. 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 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.

v. 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

i. The Supplier shall test the BCDR Plan:

  i. regularly and in any event not less than once in every Contract Year;

  ii. in the event of any major reconfiguration of the Deliverables

  iii. at any time where the Buyer considers it necessary (acting in its sole discretion).

ii. 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.

iii. 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.

iv. 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.

v. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

i. the outcome of the test;

ii. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

iii. the Supplier's proposals for remedying any such failures.

vi. 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

i. 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

i. 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 Requirements)

1. **Definitions**

1. In this Schedule, the following definitions shall apply and be supplemental to those in Joint Schedule 1 (Definitions):

4.

"Accreditation"	the assessment of the Core Information Management System in accordance with Part C

	of this Schedule by the Buyer or an independent information risk manager/professional appointed by the Buyer, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Buyer, taken in accordance with the process set out in Paragraph 4 of Part C of this Schedule, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Buyer, which is prepared by the Supplier and Approved by the Buyer in accordance with Part C of this Schedule;
“Anti-Malicious Software”	Software that scans for and identifies possible Malicious Software in the ICT Environment;
"Breach of Security"	the occurrence of: any unauthorised access to or use of the Services, the Sites, the Supplier System, and/or any information or data (including the Confidential Information and the Government Data) used by the Buyer, the Supplier or any Subcontractor in connection with this Call-Off Contract; ● the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including copies of such information or data, used by the Buyer, the Supplier and/or any Subcontractor in connection with this Call-Off Contract; and/or ● any part of the Supplier System ceasing to be compliant with the Certification Requirements, in each case as more particularly set out in the Security Requirements in Framework Schedule 1 (Specification) and the Order Form and the Security Requirements;
"Certification Requirements"	the requirements set out in Part E of this Schedule;

“CHECK Service Provider”	a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC Services required by the Paragraph 4.2 of Part C of this Schedule;
“CIMS Subcontractor”	a Subcontractor that provides or operates the whole, or a substantial part, of the Core Information Management System;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Buyer has determined in accordance with the Security Requirements;
General Security Requirements	the Security Requirements that shall apply to any Supplier and / or Subcontractor that processes Personal Data;
“Higher Risk Subcontractor”	a Subcontractor that Processes Government Data, where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Call-Off Start Date and the End Date; or (b) Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;
"IT Health Check" (ITHC)	has the meaning given Paragraph 4.2 of Part C of this Schedule;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 13.2 of Part A of this Schedule and as set out by the Supplier and Approved by the

	Buyer within the template set out in Section 23 of Appendix 1 of this Schedule;
"Information Assurance Assessment"	is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Part B of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Appendix 1 of this Schedule;
"Information Management System"	the Core Information Management System and the Wider Information Management System;
"Information Security Approval Statement"	a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data;
"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;
"Medium Risk Subcontractor"	a Subcontractor that Processes Government Data, where that data (a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Call-Off Start Date and the End Date; and (b) does not include Special Category Personal Data, other than information about the access or dietary

	requirements of the individuals concerned;
"Required Changes Register"	is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Buyer to be made to the Core Information System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in the following Paragraphs within: 2. 1.3 of Part B; ● 4 of Part C; ● 3 of Part D; together with the date on which each change shall be implemented and the date on which each change was implemented;
"Risk Management Approval Statement"	a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer;
"Risk Management Documentation"	is the information and supporting documentation that the Supplier develops and provides to the Buyer when completing section 11 of the Security Management Plan;
"Risk Management Reject Notice"	has the meaning given in Paragraph 4.8.2;
“Security Management Plan”	comprises all information required from the Supplier in order to demonstrate compliance with the Security Requirements that must be presented in the templates set out in Appendix 1;
Security Requirements	the security requirements that the Supplier and each Subcontractor must comply with during the Contract Period as set out in the this Schedule;
"Security Test"	has the meaning given Paragraphs 4 in Part C and Part D of this Schedule;

Security Working Group	the meeting led by the Buyer (or their agent) with the Supplier to discuss the Security Management Plan and any risks, issues and controls the Supplier has put into place to ensure they are delivering the Security Requirements. The timing, required attendees and periodicity of the meetings will be defined by the Buyer during implementation, but should be no less than quarterly and should include the Supplier's Staff with the relevant expertise;
"Special Category of Personal Data"	the categories of Personal Data set out in Article 9(1) of GDPR;
"Statement of Information Risk Appetite"	the document that sets-out the type and level of risk that the Buyer is prepared to accept;
"Subcontractor Security Requirements"	any Security Requirements that must be delivered by Subcontractors;
"Vulnerability Correction Plan"	has the meaning given in Paragraph Part C Paragraph 4.3.3.1 of this Schedule;
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data which have not been determined by the Buyer to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).

2. Part A Introduction

2.1. This Schedule sets out:

2.1.1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of Government Data, the Services and the Information Management System;

2.1.2. the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;

2.1.3. the Security Requirements with which the Supplier must comply, which are dependent upon the applicable Lot(s) awarded to the Supplier under the Framework Contract;

2.1.4. the tests which the Supplier shall conduct on the Information Management System during the Term;

2.1.5. the Supplier's obligations to:

2.1.5.1. return or destroy Government Data on the expiry or earlier termination of this Call-Off Contract; and

2.1.5.2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and

2.1.5.3. report Breaches of Security to the Buyer.

2.1.6. the applicable Tier of Security Requirements required to be complied with by the Supplier are summarised in Table 1 below:

Table 1:

Tier	Lot	Summary Security Requirements	Certification Requirements
1.	1	<u>General Security Requirements (Part B) plus PSC Accreditation (Part C)</u> The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request .	ISO 27001:2017 and Cyber Essentials (CE) + and PCI-DSS
2.	5, 6, 7, 20	<u>General Security Requirements (Part A) plus PSC Assurance (Part D) for Lot 20</u>	ISO 27001:2017 and CE+ and PCI-DSS

		The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request.	
3.	2, 3, 8, 9, 10, 11, 12, 13, 14	General Security Requirements (Part B)	ISO 27001:2017 and CE+
4.	4, 15, 16, 17, 18, 19	General Security Requirements (Part B) when handling Personal Data, otherwise N/A	CE

3. **Principles of Security**

3.1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently on the security of:

3.1.1. the Sites;

3.1.2. the Supplier System;

3.1.3. the Information Management System, Core information Management System and Wider Information Management System, as applicable; and

3.1.4. the Services.

3.2. Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

3.2.1. the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and

3.2.2. the security of the Information Management System.

3.3. The Supplier shall:

3.3.1. comply with the Security Requirements in this Schedule; and

3.3.2. ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements in this Schedule.

3.4. The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

3.5. The Buyer may at its sole discretion appoint an agent to act on it's behalf with regards to its engagement with the Supplier regarding the Security Requirements.

Part B General Security Requirements

1. **The Security Management Plan**

- The Security Management Plan includes details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement.

- The Supplier shall complete the Security Management Plan Template (Appendix 1) detailing how they will deliver the Security Requirements and the necessary information required for the applicable Tier(s) for the Lot(s) awarded to the Supplier. Any element that does not apply or only partially applies should be explained within the Template. If a Supplier is delivering Services in respect of more than 1 Lot, it must complete a separate Security Risk Management Template for each Lot.

- Where there has been a Variation or Change to the Services which affects any aspect of the Security Requirements, CCS and the relevant Buyers must be notified immediately in writing of this fact and the extent of its effect or believed effect on the Security Requirements and / or the Tier of the Security Requirements that the Supplier should apply to the Service (actual or potential).

- The Supplier shall complete the Security Management Plan to demonstrate and document how they comply with the Security Requirements. A draft Security Management Plan shall be made available to the Buyer prior to the Call-Off Contract Effective Date unless already Approved by the Buyer.

- The Security Management Plan should be provided to the Buyer in accordance with the Buyer's requirements and as set out within the Implementation Plan, but in any case, unless already Approved by the Buyer, this should be prior to the Service Effective Date.

- **Security Classification of Information**

o If the provision of the Services requires the Supplier to Process Government Data which is classified as: OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

- **End User Devices**

o The Supplier shall ensure that any Government Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement.

o The Supplier shall ensure that any device which is used to Process Government Data meets all of the Security Requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security

o The Supplier must ensure that their EUD's require all Supplier Staff to authenticate themselves before gaining access to the device. All the Supplier's EUD's must encrypt all data at rest using a reputable full disk encryption solution that has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement. The Supplier's EUD's must be configured to automatically lock the screen after a period of inactivity and this must be agreed with the Buyer in writing.

- **Location of Government Data**

o The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK without the Approval of the Buyer, which may be subject to conditions and that it shall comply with Joint Schedule 11 (Processing Data).

- **Vulnerabilities and Corrective Action**

o The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.

o The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability.

o The Supplier shall utilise scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

- 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 at http://nvd.nist.gov/cvss.cfm); and

- Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

o Subject to Paragraph 5.5, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

- 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

- 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

- 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

o The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 5.4 shall be extended where:

- the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 5.4 if the vulnerability becomes exploitable within the context of the Services;

- 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;

- the Buyer Approves to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan; or

- the Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Contract Period, unless otherwise Approved by the Buyer. All COTS Software should be no more than N-1 versions behind the latest software release.

- **Networking**

o The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted using TLS version 1.2 as a minimum.

- **Personnel Security**

o All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

o The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.

o The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 7.1 and 7.2 to be involved in the management and/or provision of the Services except where the Buyer Approves the involvement of the named individual in the management and/or provision of the Services.

o The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.

o The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its

Subcontractors), have their rights to access the Government Data revoked within 1 Working Day

- **Identity, Authentication and Access Control**

o The Supplier shall operate an access control regime to ensure:

  - all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

  - all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

o The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require to perform the Services under the Contract.

o The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such records available to the Buyer on request.

- **Audit and Protective Monitoring**

o The Supplier shall collect audit records which relate to security events in the Core Information Management System 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 regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access trends, any unusual

patterns of usage and/or accounts accessing higher than average amounts of Government Data.

- The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

- The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

- **Secure Architecture**

- The Supplier shall design the Core Information Management System in accordance with:

  - the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

  - the NCSC "Bulk Data Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main ; and

  - the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

- **Malicious Software**

- The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Government Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

- If Malicious Software is found, the Parties shall cooperate 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 Services to their desired operating efficiency.

- Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 11.1 shall be borne by the Parties as follows:

  - 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 the Data was provided to

the Supplier, unless the Buyer had instructed the Supplier to quarantine and check the data for Malicious Software and the Supplier had failed to do so, and

- by the Buyer, in any other circumstance.

- **Data Destruction or Deletion**

o The Supplier shall:

- prior to securely sanitising any Government Data or when requested the Supplier shall provide the Buyer with two copies of all Buyer Data in an agreed open format;
- have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;
- securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;
- securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Buyer in writing; and
- implement processes which address the CPNI and NCSC guidance on secure sanitisation.

- **Breach of Security**

o If either Party becomes aware or reasonably suspects of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

o The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

- immediately take all reasonable steps necessary to:
  - minimise the extent of actual or potential harm caused by such Breach of Security;
  - remedy such Breach of Security to the extent possible;
  - apply a tested mitigation against any such Breach of Security; and
  - prevent a further Breach of Security in the future which exploits the same root cause failure;
- as soon as reasonably practicable and, in any event, within twelve (12) hours following the Breach of Security or attempted Breach of Security, the Supplier

must provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis as required by the Buyer.

- In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the Information Management System, with this Call-Off Contract, then such remedial action shall be undertaken and completed at no additional cost to the Buyer.

- **Security Monitoring and Reporting**

- The Supplier shall:

  - monitor the delivery of assurance activities;

  - maintain and update the Security Management Plan in accordance with Paragraph 1;

  - agree a document which presents the residual security risks to inform the Buyer's decision on whether or not to give Approval to the Supplier to Process, store and transit the Government Data;

  - monitor security risk impacting upon the operation of the Service;

  - report Breaches of Security in accordance with the approved Incident Management Process; and

  - agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the Start Date of this Call-Off Contract.

Part C Accreditation requirements

1. **This Part sets out:**

- The Accreditation arrangements that the Supplier must implement and comply with when providing the Services and performing its other obligations under this Call-Off Contract. These are required to ensure the security of the Government Data, the ICT Environment, the Services and the Information Management System, which are in addition to the requirements set-out in Parts A, B and E and Appendix 1 and 2 of this Schedule.

- To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise.

- The Supplier shall provide access to the Supplier Staff responsible for information assurance and the Buyer shall provide access to its Personnel responsible for information assurance, at reasonable times upon reasonable written notice.

- **Information Management System**

  - The Information Management System comprises the Core Information Management System and the Wider Information Management System.

  - The Buyer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Buyer to make such determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Subcontractor to Process Government Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Buyer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

- The Supplier shall reproduce the Buyer's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

- Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the

Wider Information Management System shall be notified and processed in accordance with Clause 24 of the Core Terms (Changing the contract).

- **Statement of Information Risk Appetite and Security Requirements**

o The Supplier acknowledges that the Buyer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services ("**Statement of Information Risk Appetite**").

o The Buyer's Security Requirements in respect of the Core Information Management System shall be set out in Appendix 1 (below).

- **Accreditation of the Core Information Management System**

o The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 4.

o The Supplier acknowledges that the purpose of Accreditation is to ensure that:

  - the Security Management Plan accurately represents the Core Information Management System;
  - the Accreditation Plan, if followed, provides the Buyer with sufficient confidence that the CIMS will meet the requirements of the Security Requirements and the Statement of Risk Appetite; and
  - the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Security Requirements.

o The Accreditation shall be performed by the Buyer or by representatives appointed by the Buyer.

o In addition to any obligations imposed by Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Subcontractors, from the Call-Off Contract Start Date.

o By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Buyer the risk management documentation for the Core Information Management System, which shall be subject to approval by the Buyer in accordance with, Part B Paragraph 5 (the "**Security Management Plan**").

o The Supplier must provide, by the date by which the Supplier is required to have received a Risk Management Approval Statement from the Buyer together with:

  - details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed

in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.8.1.

- a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;

- a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Services, processes associated with the delivery of the Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to extent that it is under the control of or accessed the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; and

- unless such requirement is waived by the Buyer, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, 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 IT, Information and data (including the Confidential Information of the Buyer and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Call-Off Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services including:

    - the Required Changes Register;

    - evidence that the Supplier and each applicable Subcontractor is compliant with the Certification Requirements;

    - a Personal Data Processing Statement; and

    - the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 3.2.

o To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:

- access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and

- such other information and/or documentation that the Buyer or its authorised representatives may reasonably require, to enable the Buyer to establish that the

Core Information Management System is compliant with the Security Management Plan.

- The Buyer shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:
  - a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Buyer is satisfied that the identified risks to the Core Information Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer; or
  - a rejection notice stating that the Buyer considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why (**"Risk Management Rejection Notice"**).
- If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:
  - address all of the issues raised by the Buyer in such notice;
  - update the Security Management Plan, as appropriate, and
  - notify the Buyer that the Core Information Management System is ready for an Accreditation Decision.
- If the Buyer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.
- Subject to Paragraph 4.10, the process set out in Paragraphs 4.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Call-Off Contract.
- The Supplier shall not use the Core Information Management System to Process Government Data prior to receiving a Risk Management Approval Statement.
- The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this Paragraph 4 and the Buyer shall review the

Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.9.

- The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
  - a significant change to the components or architecture of the Core Information Management System;
  - a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;
  - a change in the threat profile;
  - a Subcontractor failure to comply with the Core Information Management System code of connection;
  - a significant change to any risk component; and/or
  - a significant change in the quantity of Personal Data held within the Core Information Management System.
- Where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual:
  - a proposal to change any of the Sites from which any part of the Services are provided; and
  - an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and
  - update the Required Changes Register and provide the updated Required Changes Register to the Buyer for review and Approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Buyer.
- If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Buyer, such failure shall constitute a material Default and the Supplier shall:
  - immediately cease using the Core Information Management System to Process Government Data until the Default is remedied, unless directed otherwise .by the Buyer in writing and then it may only continue to Process Government Data in accordance with the Buyer's written directions; and
  - where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Buyer and, should the Supplier fail to remedy the Default within such timescales, the Buyer may terminate this Call-Off Contract with

immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms

- The Supplier shall review each Change request against the Security Management Plan to establish whether the documentation would need to be amended should such Change request be agreed and, where a Change request would require an amendment to the Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change request for consideration and Approval by the Buyer.

- The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Buyer as part of the Accreditation process.

- **Security Testing**

- The Supplier shall, at its own cost and expense:

- procure testing of the Core Information Management System by a CHECK Service Provider (an "**IT Health Check**"):

    - prior to it submitting the Security Management Plan to the Buyer for an Accreditation Decision;

    - if directed to do so by the Buyer; and

    - once every 12 Months during the Call-Off Contract Period:

    - conduct vulnerability scanning and assessments of the Core Information Management System Monthly;

    - conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Subcontractors of a critical vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and

        - conduct such other tests as are required by:

        - any Vulnerability Correction Plans;

        - the ISO27001 certification requirements;

        - the Security Management Plan; and

        - The Buyer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,

    (each a "**Security Test**").

- 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, and in any case within 10 Working Days, after completion of each Security Test.

- In relation to each IT Health Check, the Supplier shall:

  - agree with the Buyer the aim and scope of the IT Health Check;

  - promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Buyer with a copy of the IT Health Check report

  - in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

  - prepare a remedial plan for approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

    - how the vulnerability will be remedied;

    - the date by which the vulnerability will be remedied;

    - the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

    - comply with the Vulnerability Correction Plan; and

    - conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

- The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.

- The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 5.3, 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, and in any case no later than 10 Working Days, after completion of each Security Test.

- The Buyer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Buyer Security Tests**"). The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature and purpose of the Buyer Security Test.

- The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.

- The Buyer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Buyer Security Test causes Supplier Non-Performance, the Buyer Security Test shall be treated as an Authority Cause for the purposes of Clause 5.1 of the Core Terms, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Buyer Security Test.

- Without prejudice to the provisions of Paragraph 5.3, where any Security Test carried out pursuant to this Paragraph 5 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 Core Information Management System and/or 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 Approval, the Supplier shall implement such changes to the Core Information Management System and/or 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.

- If the Buyer unreasonably withholds its Approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 5.9 above, the Supplier shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:

  - has arisen as a direct result of the Buyer unreasonably withholding its Approval to the implementation of such proposed changes; and

  - would have been avoided had the Buyer given its Approval to the implementation of such proposed changes.

- For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Security Requirements and/or any obligation in this Call-Off Contract, the Supplier shall effect such change at its own cost and expense.

- If any repeat Security Test carried out pursuant to Paragraph 5.3 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

- The Supplier shall, by 31 March of each Financial Year during the Call-Off Contract Period, provide to the Buyer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:

  - the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Call-Off Contract; and

- the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.

- Vulnerabilities and Corrective Action

- In addition to the requirements within Part B, the Supplier shall:

- implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;

- promptly notify NCSC of any actual or sustained attempted Breach of Security;

- ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

- ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Call-Off Contract Period;

- pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;

- from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent Month during the Call-Off Contract Period, provide the Buyer with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the 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 and any failure to comply with the timescales set out in Part B Paragraph 5.4 for applying patches to vulnerabilities in the Core Information Management System;

- propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;

- 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 Core Information Management System); and

- 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 Core Information Management System and provide initial indications of possible mitigations.

- If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Part B Paragraph 5.4, the Supplier shall immediately notify the Buyer.

- If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Part B Paragraph 5.3, such failure shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect

by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

PART D Assurance requirements

1. This Part D sets out the Assurance arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Government Data and the Information Management System.

. The Supplier must comply with the Assurance arrangements in addition to the other Security Requirements as set out within Parts A and B and E of this Schedule and Appendix 1 (Security Management Plan).

24 Information Security Approval Statement

. The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Sub-contractors from the Call-Off Start Date.

. The Supplier may not use the Information Management System to Process Government Data unless and until:

() the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider in accordance with Paragraph 4; and

() the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 2.

. The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule and the Call-Off Contract in order to ensure the security of the Government Data and the Information Management System.

. The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which comprises:

() an Information Assurance Assessment;

() the Required Changes Register;

() the Personal Data Processing Statement; and

() the Incident Management Process.

. The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

() an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or

() a rejection notice which shall set out the Buyer's reasons for rejecting the Security Management Plan.

. If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.

. The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:

() access to the Supplier Staff;

() access to the Information Management System to Audit the Supplier and its Subcontractors' compliance with this Call-Off Contract;

() such other information and/or documentation that the Buyer or its authorised representatives may reasonably require;

() assistance to the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan; and

() the Supplier shall provide the access required by the Buyer in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

25 Compliance Reviews

. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

() a significant change to the components or architecture of the Information Management System;

() a new risk to the components or architecture of the Service;

() a vulnerability to the components or architecture of the Service which is classified '**Medium**', '**High**', '**Critical**' or '**Important**' in accordance with the classification methodology set out in Paragraph 5 of Part B to this Schedule;

() a change in the threat profile;

() a significant change to any risk component;

() a significant change in the quantity of Personal Data held within the Service;

() a proposal to change any of the Sites from which any part of the Services are provided; and/or

() an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.

. Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Buyer for review and Approval.

. Where the Supplier is required to implement a change, including any change to the Information Management System the Supplier shall effect such change at its own cost and expense.

26 Security Testing

. The Supplier shall, at its own cost and expense procure and conduct:

() testing of the Information Management System by a CHECK Service Provider ("**ITHC**"); and

() such other security tests as may be required by the Buyer; and

() the Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12 Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.

. In relation to each ITHC, the Supplier shall:

() agree with the Buyer the aim and scope of the ITHC;

() promptly, and no later than 10 Working Days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;

() in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

() prepare a remedial plan for Approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:

() how the vulnerability will be remedied;

() the date by which the vulnerability will be remedied; and

() the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

() comply with the Vulnerability Correction Plan; and

() conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

. The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.

. If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique] that has the potential to affect the security of the Information Management System, the Supplier shall within days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:

() propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and

() where and to the extent applicable, 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 Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

. The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.

. The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 5 of Part B to this Schedule.

Part E Certification requirements

Certification Requirements

1. Supplier Requirements

1.1. The Supplier shall as applicable to the Lot and the associated Security Tier, ensure, at all times during the Call-Off Contract Period, that it is certified as compliant with:

1.1.1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

1.1.2. Cyber Essentials or Cyber Essentials PLUS as applicable to the Lot and Security Tier of the Service, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme), and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier or the relevant Subcontractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Government Data.

2. **Payment Card Industry Data Security Standard (PCI DSS) Compliance**

2.1. All Suppliers and / or Subcontractors that are a payment processor must be, and remain, appropriately certified according to the Payment Card Industry Data Security Standard requirements throughout the term of the Contract

2.2. Where the Supplier and / or Subcontractor intends to accept payments, restricted to at sale only, by debit/credit card the Supplier and / or Subcontractor must have either:

2.2.1. been certified by a Qualified Security Assessor being compliant with the PCI DSS version 1.1;

2.2.2. completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the Client promptly in writing of any changes in the Contractor's certification.

2.3. The Supplier / Subcontractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the Buyer with written evidence of compliance annually.

2.4. The Supplier / Subcontractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.

2.5. The Supplier / Subcontractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.

2.6. The Supplier / Subcontractor must be responsible for the security of all cardholder Data in their possession and must protect data by the card scheme industry standard on an annual basis and provide the Buyer access hosted environment and data when necessary.

2.7. The Supplier / Subcontractor must notify the Buyer and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.

2.8. The Supplier / Subcontractor must indemnify the Buyer, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, Losses, whatsoever incurred by it or them arising out of or in connection with the Supplier's non-compliance with, or breach of, the PCI DSS or breach of Cardholder Data security.

2.9. The Supplier / Subcontractor must cease taking payments, by Debit Card / Credit Card, on behalf of the Buyer in the event that the Supplier becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

3. **Subcontractor Requirement**

3.1. Notwithstanding anything else in this Contract, a CMIS Subcontractor shall be treated for all purposes as a Key Subcontractor.

3.2. In addition to the obligations contained in Joint Schedule 6 (Key Subcontractors), the Supplier must ensure that the Key Subcontract with each CIMS Subcontractor.

3.3. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Call-Off Schedule 9 (Security Requirements);

3.3.1. provides for the Buyer to perform Accreditation of any part of the Core Information Management System that the CIMS Subcontractor provides or operates which is not otherwise subject to Accreditation under this Call-Off Schedule 6 (Security Requirements).

3.4. The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant, and the Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data, with either:

3.4.1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

3.4.2. Cyber Essentials PLUS, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme),

3.5. The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme).

3.6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:

3.6.1. immediately ceases using the Government Data; and

3.6.2. procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with Security Requirements.

3.7. The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

Appendix 1

Security Management Plan Template

DRS Call-Off Schedule 9 (Appendix 1)

Security Management Plan Template

[Lot/Service]

[Supplier Name]

Author:

Owner:

Date:

Version:

[Guidance Note: *The Supplier shall complete this Security Management Plan Template in as much detail as possible and if any provision does not apply to the Supplier, it must explain why.*]

1 Executive Summary

<This section should contain a brief summary of the business context of the Supplier System [including any Subcontractor system], any key Information Assurance controls, assurance work done, off-shoring considerations and significant residual risks that need acceptance by the Buyer.>

1.1 List of Contents

1.1 Security Requirements Change History

Version Number	Date of Change	Change made by	Nature and reason for change

1.2 References, Links and Dependencies

This Security Management Plan Template relies upon the supporting information and assurance provided by the following documents:

ID	Document Title	Reference	Date
•			
•			

2 System Description

3 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

4 Organisational Ownership/Structure

< Who owns the system, operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the Buyer and Buyer governance *board as per their Call-Off Contract.>*

5 Information assets and flows

<The information assets processed by the system, which should include a simple high level diagram on one page, as well as a list of the type and volumes of data that will be processed, managed and stored within the Supplier System. If Personal Data is processed, please include the fields used such as name, address, department DOB, NI number etc. in Annex 1 of Joint Schedule 11 (Processing Data).>

6 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will need to be included here>

7 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, the security clearance level requirements of those users should be included.>

8 Locations

<Detail where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be specified, as well as any off-shoring considerations.>

9 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

10 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

11 Accreditation/Assurance Scope

<This section should describe the scope of the Accreditation/Assurance for the system (applicable to Tier 1 and Tier 2 Security Requirements). The scope of the assurance assessment should be clearly indicated, expressly including those components upon which reliance is placed but where assurance will not be undertaken, e.g. a cloud hosting service. A logical diagram should be inserted here along with a brief description of the components.>

12 Risk appetite

<A risk appetite should be agreed with the Buyer's Head of IA and detailed here.>

13 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive Personal Data the loss of which would be severely damaging to individuals, embarrassing to HMG and could make HMG liable to an Information Commissioner Office investigation) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

14 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen. It should contain a prioritised list of the output of the formal information risk using plain English language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

15 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further informati
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC

C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part o

16 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated (above), after all controls have been applied and verified, should be listed with actions and timescales included.>

17 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the Contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include as a minimum:

a) *information risk management and timescales and triggers for a review;*

b) *contractual patching requirements and timescales for the different priorities of patch;*

c) *protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;*

d) *configuration and change management;*

e) *incident management;*

f) *vulnerability management;*

g) *user access management; and*

h) *data sanitisation and disposal.>*

18 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

19 Third Party Subcontractors/Suppliers/Products

< Please provide a table of any third party subcontractor/suppliers and products that you are using to deliver your Services for the Buyer. Please also include the location of where they are Processing or storing the Data and what function they are performing as well as how they comply with the contractual security requirements. >

20 Physical Security

<Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail the measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Also include details of any automated access controls, alarms and CCTV coverage and details of the maintenance schedule of these security controls.>

21 Major Hardware and Software and end of support dates

< Please complete a table listing the end of support dates for hardware and software products and components. For example:>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
er Host	HP XXXX	Feb 2020/ March 2022	

22 Incident Management Process

<The Suppliers' process, as agreed with the Buyer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to CCS / the Buyer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

23 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

24 Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Docu upda
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Buyer's name	11/11/2018	Jul-2

25 Personal Data Processing Statement

<The Supplier shall complete Annex 1 of Joint Schedule 11 (Processing Data) detailing: (i) the types of Personal Data which the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (iii) the nature and purpose of such Processing; (iv) the locations at which the Supplier and/or its Subcontractors Process Buyer Data; and, (v) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Buyer Data against a Security Breach including a Personal Data Breach.>

-:-

26 Annex A: ISO27001 and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

27 Annex B: Cloud Security Principles assessment

<A spreadsheet may be attached>

28 Annex C: Protecting Bulk Data assessment if required by the Buyer

<A spreadsheet may be attached>

29 Annex D: Latest ITHC report and Vulnerability Correction Plan

Appendix 2

ACCREDITATION - CORE INFORMATION MANAGEMENT SYSTEM DIAGRAM

[Guidance Note: To be completed in discussions with Supplier]

Call-Off Schedule 10 (Exit Management)

2. **Definitions**

i. 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 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 in connection with the Deliverables but which are also used by the Supplier 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.

3. **Supplier must always be prepared for contract exit**

i. The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

ii. During the Contract Period, the Supplier shall promptly:

i. 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

ii. create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("**Registers**").

iii. The Supplier shall:

i. ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

ii. 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.

iv. Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

4. **Assisting re-competition for Deliverables**

i. 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 (the "**Exit Information**").

ii. 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.

iii. 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).

iv. 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.

5. **Exit Plan**

i. The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

ii. 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.

iii. The Exit Plan shall set out, as a minimum:

i. a detailed description of both the transfer and cessation processes, including a timetable;

ii. how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

iii. 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;

iv. 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;

v. 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;

vi. proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

vii. proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

viii. proposals for the disposal of any redundant Deliverables and materials;

ix. how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

x. any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

iv. The Supplier shall:

i. maintain and update the Exit Plan (and risk management plan) no less frequently than:

1. every six (6) months throughout the Contract Period; and

2. no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

3. 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;

4. 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

ii. jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

v. 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.

vi. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

6. **Termination Assistance**

i. 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 (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:

i. the nature of the Termination Assistance required; and

ii. 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.

ii. 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:

i. no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

ii. 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.

iii. 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.

iv. 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).

7. **Termination Assistance Period**

i. Throughout the Termination Assistance Period the Supplier shall:

i. 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;

ii. 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;

iii. use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

iv. 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;

v. at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

vi. seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

ii. 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.

iii. 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, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

8. **Obligations when the contract is terminated**

i. The Supplier shall comply with all of its obligations contained in the Exit Plan.

ii. 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:

i. vacate any Buyer Premises;

ii. 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;

iii. 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:

1. such information relating to the Deliverables as remains in the possession or control of the Supplier; and

2. 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.

iii. 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.

9. **Assets, Sub-contracts and Software**

i. Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

i. terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

ii. (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

ii. 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:

i. which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

ii. which, if any, of:

1. the Exclusive Assets that are not Transferable Assets; and

2. the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

iii. 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.

iii. 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.

iv. 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.

v. 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:

i. 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

ii. procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

vi. 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.

vii. The Buyer shall:

i. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

ii. 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.

viii. 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.

ix. 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.

10. **No charges**

i. 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.

11. **Dividing the bills**

i. 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:

i. the amounts shall be annualised and divided by 365 to reach a daily rate;

ii. 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

iii. the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1. **Definitions**

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

"Delay"	1. a delay in the Achievement of a Milestone by its Milestone Date; or

	2. a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	1. an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	• a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	• has the meaning given to it in Paragraph 7.1;

- **Agreeing and following the Implementation Plan**
  - A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan [**Insert** number of days] days after the Call-Off Contract Start Date.
  - The draft Implementation Plan:
    - must cover all aspects of the Services and the Supplier's obligations under this Call-Off Contract, including the requirements set out in Call-off Schedule 9 (Security Management);
    - must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and
    - it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.
  - Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
  - The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

- The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

- **Reviewing and changing the Implementation Plan**
  - Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.
  - The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.
  - Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.
  - Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

- **Security requirements before the Start Date**
  - The Supplier shall note that it is incumbent upon them to understand and plan for the implementation of the Security Requirements applicable to the provision of the Services as detailed in Call-Off Schedule 9 (Security Management) which must be satisfied and in place before the Call-Off Start Date. The Supplier shall ensure that the applicable Security Requirements are reflected in their Implementation Plans.
  - The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's personnel security requirements set out in Paragraph 4.1 of Call-Off Schedule 9 (Security Management)-.
  - The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.
  - The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.
  - The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has

been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

- If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

- **What to do if there is a Delay**

  - If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:
    - notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;
    - include in its notification an explanation of the actual or anticipated impact of the Delay;
    - comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and
    - use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

- **Compensation for a Delay**

  - If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:
    - the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;
    - Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:
      - the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

- the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

- the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;
- no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and
- Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

Call-Off Schedule 14 (Service Levels)

1. **Definitions**
   - In 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 Credits"	• any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	• has the meaning given to it in the Order Form;
x"Service Level Failure"	• means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	• shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	• shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

- **What happens if you don’t meet the Service Levels**
  - The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
  - The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier’s failure to meet any Service Level Performance Measure.
  - 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.
  - A Service Credit shall be the Buyer’s exclusive financial remedy for a Service Level Failure except where:

- the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
- the Service Level Failure:
  - exceeds the relevant Service Level Threshold;
  - has arisen due to a Prohibited Act or wilful Default by the Supplier;
  - results in the corruption or loss of any Government Data; and/or
  - results in the Buyer being required to make a compensation payment to one or more third parties; and/or
- the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

o 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:

- 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;
- 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; and
- there is no change to the Service Credit Cap.

● **Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

o any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

o the Buyer shall (subject to the Service Credit Cap) 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 and Service Credits

1. Service Levels

If the level of performance of the Supplier:

i. is likely to or fails to meet any Service Level Performance Measure; or

ii. 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:

- 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;
- instruct the Supplier to comply with the Rectification Plan Process;
- if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- 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. Service Credits

i. The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

ii. Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Accurate and timely billing of Buyer	Accuracy /Timelines	at least 98% at all times	98% - 100%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Access to Buyer support	Availability	at least 98% at all times	98% - 100%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure

The Service Credits shall be calculated on the basis of the following formula:

Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance)	=	x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)	=	23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

Part B: Performance Monitoring

3. **Performance Monitoring and Performance Review**

i. 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.

ii. 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 this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

i. for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

ii. a summary of all failures to achieve Service Levels that occurred during that Service Period;

iii. details of any Critical Service Level Failures;

iv. for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

v. the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

vi. such other details as the Buyer may reasonably require from time to time.

iii. 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:

i. take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

ii. be attended by the Supplier's Representative and the Buyer's Representative; and

iii. 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.

iv. 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.

v. 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 and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

i. 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.

Call-Off Schedule 15 (Call-Off Contract Management)

1. Definitions

i. 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

i. 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.

ii. 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.

iii. 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**

i. The Supplier's Contract Manager's shall be:

i. 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;

ii. 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;

iii. able to cancel any delegation and recommence the position himself; and

iv. replaced only after the Buyer has received notification of the proposed change.

ii. The Buyer may provide revised instructions to the Supplier's Contract Manager's 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.

iii. 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

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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**

i. Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

ii. The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

i. the identification and management of risks;

ii. the identification and management of issues; and

iii. monitoring and controlling project plans.

iii. The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

iv. 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:

.]

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