

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

Order Form

CALL-OFF REFERENCE: SR1623453311
SUPPLIER'S REFERENCE: [REDACTED]

THE BUYER: **His Majesty's Revenue and Customs**

BUYER ADDRESS 100 Parliament Street, London SW1A 2BQ

THE SUPPLIER: Pegasystems Limited

SUPPLIER ADDRESS: 23 Forbury Road, Reading, Berkshire, RG1 3JH

REGISTRATION NUMBER: 02883981

DUNS NUMBER: [REDACTED]

SID4GOV ID: N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 25th March 2024

It's issued under the Framework Contract with the reference number RM6194 for the provision of Back Office Software.

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.
 - Joint Schedule 1(Definitions and Interpretation) RM6194
2. The following Schedules in equal order of precedence:
 - Joint Schedules for **RM6194**
 - [Joint Schedule 2 \(Variation Form\)](#)
 - [Joint Schedule 3 \(Insurance Requirements\)](#)

- [Joint Schedule 4 \(Commercially Sensitive Information\)](#)
 - [Joint Schedule 6 \(Key Subcontractors\)](#)
 - [Joint Schedule 7 \(Financial Difficulties\)](#)
 - [Joint Schedule 9 \(Minimum Standards of Reliability\)](#)
 - [Joint Schedule 10 \(Rectification Plan\)](#)
 - [Joint Schedule 11 \(Processing Data\)](#)
 - [Joint Schedule 12 \(Supply Chain Visibility\)](#)
 - Call-Off Schedules for **RM6194**
 - [Call-Off Schedule 1 \(Transparency Reports\)](#)
 - [Call-Off Schedule 2 \(Staff Transfer\)](#)
 - [Call-Off Schedule 3 \(Continuous Improvement\)](#)
 - [Call-Off Schedule 5 \(Pricing Details\)](#)
 - [Call-Off Schedule 7 \(Key Supplier Staff\)](#)
 - [Call-Off Schedule 8 \(Business Continuity and Disaster Recovery\)](#)
 - [Call-Off Schedule 9 \(Security\)](#)
 - [Call-Off Schedule 10 \(Exit Management\)](#)
 - [Call-Off Schedule 14 \(Service Levels\)](#)
 - [Call-Off Schedule 15 \(Call-Off Contract Management\)](#)
 - [Call-Off Schedule 16 \(Benchmarking\)](#)
 - [Call-Off Schedule 18 \(Background Checks\)](#)
 - [Call-Off Schedule 20 \(Call-Off Specification\)](#)
 - [Call-Off Schedule 23 \(Supplier-Furnished Terms\)](#)
3. CCS Core Terms (version 3.0.10)
- [Joint Schedule 5 \(Corporate Social Responsibility\)](#) RM6194 applicable to the extent policy in place and being made available. Policy available at:
 - <https://www.pega.com/about/leadership/governance/slavery-and-human-trafficking-statement>

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.

Parties agree the following:

This Call-Off replaces, terminates and supersedes previous agreement with Pega contract reference CR-52545, CR-59229, CR-64950, CR-80860, CR-67557, CR-85640, CR-82084 as of Start Date.

CALL-OFF SPECIAL TERMS

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

Special Term 1

Terms included:

[Additional Schedule HMRC Specific Terms](#)

[Additional Schedule Professional Services](#)

Special Term 2.

Core Terms:

Following clauses are deleted; 3.2.3, 3.2.11, 4.9, 4.10

Special Term 3.

Core Terms:

Following clauses are amended:

- 9.1 9.1 Each Party keeps ownership of its own Existing IPR. The Supplier gives the Buyer a, royalty-free, irrevocable, transferable within His Majesty's Government, non-exclusive licence to use the Supplier's Existing IPR to enable it to both:
- a) receive and use the Deliverables; and,
 - b) make use of the deliverables provided by a Replacement Supplier.

Supplier owns all right, title and interest to the Supplier Software and permits Buyer to use during the term of this Call-Off.

"Software" means the Supplier software listed in this Call-Off, including any enhancements, updates, upgrades, modifications, or other releases provided to Buyer.

Additional sub-clause 10.2.1a

The Call-Off shall survive any termination by CCS of the Framework under clause 10.2.1

- 10.2.2 Buyer has the right to terminate this Call-Off Contract without reason by giving the Supplier not less than 365 days' written notice, provided that Buyer cannot exercise such right prior to the second anniversary of this Call-Off Start Date and therefore cannot be exercised prior to 1st April 2026. Therefore, the initial term of 3 years and associated fees remain committed.

CALL-OFF START DATE: **1st April 2024**

CALL-OFF EXPIRY DATE: **31st March 2027**

CALL-OFF INITIAL PERIOD: **3 Years**

CALL-OFF EXTENTIONS: Two (2) optional Twelve (12) month extensions (at the discretion of the Authority)

<p>Indexation</p>	<p>[Redacted]</p>
<p>Delivery & Acceptance</p>	<p>[Redacted]</p>
<p>Credit for Services</p>	<p>[Redacted]</p>

During the Initial Term, Buyer may purchase additional usage and capacity as follows:

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

- a. Purchases of additional usage and/or capacity will be exercised by sending written notice to Pegasystems and entering into a written amendment. The term for any additional usage and/or capacity purchased will be co-terminus with the Term of this Schedule. The terms of the Agreement will govern any purchase order, and any terms that may be printed on the purchase order will be of no force and effect.
- b. If Buyer exceeds any of its usage rights, Pegasystems will have the right to invoice Buyer for all additional usage and/or capacity per the pricing set forth in the tables above. Period will be co-terminus with the Call Off Expiry Date.

In the event HMRC wish to reduce their usage of DX/API or Collections cases in a Renewal Term, the following fees will apply from the point of Renewal.

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

By way of invoice. Annual fee payable annually in advance

BUYER'S INVOICE ADDRESS:

HMRC Invoice Processing Centre,
PO BOX 2092, J Spur, Barrington Road
Worthing, BN12 9AN

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]

Commercial Contract Manager

BUYER'S ENVIRONMENTAL POLICY

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

BUYER'S SECURITY POLICY

A Baseline Personnel Security Standard (BPSS) pack will be needed for relevant supplier persons delivering consulting services within the governance of this contract; Security Check (SC) will be required for any Production System access as agreed between the parties.

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

Account Executive

[REDACTED]

[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

Account Executive

[REDACTED]

[REDACTED]

KEY STAFF

See details in Call Off Schedule 7 Key Supplier Staff

KEY SUBCONTRACTOR(S)

None

Framework Ref: RM6194

Project Version: v1.0

Model Version: v3.1

COMMERCIALLY SENSITIVE INFORMATION

See details in Joint Schedule 4 Commercially Sensitive Information

SERVICE CREDITS

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

ADDITIONAL INSURANCES

Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

Social Value commitments and collaboration is to be conducted under Strategic Supplier Relationship Management (SSRM) and the Supplier is expected to cooperate with SSRM to ensure a plan is followed and actions agreed.

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

Joint Schedule 2 (Variation Form)

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

Contract Details	
This variation is between:	[delete] as applicable: CCS / Buyer] (" CCS " " the Buyer ") And [insert] name of Supplier] (" the Supplier ")
Contract name:	[insert] name of contract to be changed] (" the Contract ")
Contract reference number:	[insert] contract reference number]
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
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: <ul style="list-style-type: none"> [CCS/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 must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete]** as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

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

Signature	
Date	
Name (in Capitals)	
Address	

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

Signature	
Date	
Name (in Capitals)	
Address	

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

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

5. Making sure you are insured to the required amount

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

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:
 - 1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);
 - 1.2 public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and
 - 1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and
 - 1.4 product liability insurance with cover (for a single event or series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Item(s)	Duration of Confidentiality
1	[Redacted]	[Redacted]
2	[Redacted]	[Redacted]
3	[Redacted]	[Redacted]
4	[Redacted]	[Redacted]
5	[Redacted]	[Redacted]
6	[Redacted]	[Redacted]
7	[Redacted]	[Redacted]

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

- 1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)
- 1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
 - 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

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

- 3.1 The Supplier:
 - 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
 - 3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

- 3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
- 3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

- 4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;
- 4.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

- 4.1.4 not make deductions from wages:
 - (a) as a disciplinary measure
 - (b) except where permitted by law; or
 - (c) without expressed permission of the worker concerned;
- 4.1.5 record all disciplinary measures taken against Supplier Staff;
and
- 4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

- 5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
- 5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;
- 5.1.3 ensure that use of overtime used responsibly, taking into account:
 - (a) the extent;
 - (b) frequency; and
 - (c) hours worked;

by individuals and by the Supplier Staff as a whole;

- 1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
- 1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
 - 1.3.1 this is allowed by national law;
 - 1.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
appropriate safeguards are taken to protect the workers' health and safety; and
 - 1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.
- 1.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

2. Sustainability

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

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

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

- 1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- 1.2 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.
- 1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer 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:
 - 1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 1.3.3 the proposed Key Subcontractor employs unfit persons.
- 1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 1.4.3 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;
 - 1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - 1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

- 1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.
- 1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
 - 1.5.1 a copy of the proposed Key Sub-Contract; and
 - 1.5.2 any further information reasonably requested by CCS and/or the Buyer.
- 1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
 - 1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);
 - 1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - 1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to

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

Joint Schedule 7 (Financial Difficulties)

1. Definitions

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

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: <ul style="list-style-type: none"> a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: <ul style="list-style-type: none"> i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;

	<p>ii) non-payment by the Monitored Company of any financial indebtedness;</p> <p>iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or</p> <p>iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company</p> <p>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;</p>
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier or any Key Subcontractor
"Rating Agencies"	6 the rating agencies listed in Annex 1.

2. When this Schedule applies

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

2.2 The terms of this Schedule shall survive:

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

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

3. What happens when your credit rating changes

- 3.1 The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.
- 3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.
- 3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with 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].

3.4 The Supplier shall:

- 3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and
- 3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

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

4. What happens if there is a financial distress event

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

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

4.2.1 rectify such late or non-payment; or

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

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

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

4.3.2 where CCS 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:

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

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

4.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to

CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

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

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

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

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

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

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.4.6.

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

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

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

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

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

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

6. What happens If your credit rating is still good

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

- 6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and
- 6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

ANNEX 1: RATING AGENCIES

Moody's - Buyer Nominated

Dunn & Bradstreet – Supplier Nominated

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
██████████	■
[Key Subcontractor]	

Joint Schedule 9 (Minimum Standards of Reliability)

1. Standards

1.1 No Call-Off Contract with an anticipated contract value in excess of £20 million (excluding VAT) shall be awarded to the Supplier if it does not show that it meets the minimum standards of reliability as set out in the OJEU Notice (“**Minimum Standards of Reliability**”) at the time of the proposed award of that Call-Off Contract.

1.2 CCS shall assess the Supplier’s compliance with the Minimum Standards of Reliability:

1.2.1 upon the request of any Buyer; or

1.2.2 whenever it considers (in its absolute discretion) that it is appropriate to do so.

1.3 In the event that the Supplier does not demonstrate that it meets the Minimum Standards of Reliability in an assessment carried out pursuant to Paragraph 1.2, CCS shall so notify the Supplier (and any Buyer in writing) and the CCS reserves the right to terminate its Framework Contract for material Default under Clause 10.4 (When CCS or the Buyer can end this contract).

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan		
Details of the Default:	[Guidance: Explain the Default, with clear schedule and clause references as appropriate]	
Deadline for receiving the [Revised] Rectification Plan:	[add date (minimum 10 days from request)]	
Signed by [CCS/Buyer] :		Date: <input type="text"/>
Supplier [Revised] 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	<input checked="" type="checkbox"/> 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)

Status of the Controller

1. 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. A Party may act as:
 - (a) “Controller” in respect of the other Party who is “Processor”;
 - (b) “Processor” in respect of the other Party who is “Controller”;
 - (c) “Joint Controller” with the other Party;
 - (d) “Independent Controller” of the Personal Data where there 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

2. 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.
3. The Processor shall notify the Controller with undue delay if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, for the processing of Client Personal Data in the context of providing the Supplier services in such a manner to ensure a level of security appropriate to the risk to the Client Personal Data when it is processed by the Supplier
- (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) Buyer has granted its prior written consent under Call-Off Schedule 23 – Supplier Terms to Supplier to process Personal Data for Permitted Purposes (which the Buyer may have encrypted) within and subject to access controls for environments and controls outside of the UK.
 - (ii) The Personal Data will be stored in the selected Deployment Region. The processing and access to Personal Data shall only take place for Permitted Purposes, unless with prior written agreement of the Buyer.
 - (iii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

- (iv) the Data Subject has enforceable rights and effective legal remedies;
 - (v) 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
 - (vi) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller with undue delay if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
8. 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 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) providing without unreasonable delay:
- (a) the Controller with full details and copies of the complaint, communication or request;

- (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
 - (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
12. Buyer grants to Supplier the general authorization to engage the services of its Affiliates and Subprocessors set forth in <https://www.pega.com/subprocessors> to provide the Pega Cloud complying with Schedule 9. Any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) hold a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
 - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
14. The Relevant Authority may, at any time on not less than 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).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 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

16. 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 GDPR Article 26.

Independent Controllers of Personal Data

17. 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.
18. 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.
19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 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.
20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
21. The Parties shall only provide Personal Data to each other:
 - (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.
24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
 - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
 - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

- (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 26. 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*).
- 27. 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*).
- 28. Notwithstanding the general application of paragraphs 2 to 15 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 16 to 27 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: ██████████

1.2 The contact details of the Supplier's Data Protection Officer are: ██████████

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the Personal Data required for any given application.</p>
Duration of the Processing	Data will be processed for the duration of this contract and will be extended should any contractual extension options be exercised.
Nature and purposes of the Processing	<p>Buyer agrees that Supplier may process Client Personal Data for (i) providing Subscription Services detailed in this Schedule; (ii) disclosures to Subprocessors; and (iii) as authorized by Data Protection Law or other applicable law (the "Permitted Purposes"). Supplier is reliant on Buyer's representations of the extent to which Supplier is authorized to process Client Personal Data</p> <p>██████████</p>

	<p>[Redacted content]</p>
--	---------------------------

Joint Schedule 12 (Supply Chain Visibility)

1. 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.

2. Visibility of Sub-Contract Opportunities in the Supply Chain

2.1 The Supplier shall:

- 2.1.1 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;
- 2.1.2 within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;
- 2.1.3 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;

- 2.1.4 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
 - 2.1.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.
- 2.2 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.
- 2.3 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.
- 2.4 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.

3. Visibility of Supply Chain Spend

- 3.1 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:
- (a) the total contract revenue received directly on the Contract;
 - (b) the total value of sub-contracted revenues under the Contract (including revenues for non-SMEs/non-VCSEs); and
 - (c) the total value of sub-contracted revenues to SMEs and VCSEs.
- 3.2 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.

- 3.3 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



Supply Chain Information
Report templat

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	Performance against all SLAs and KPIs. Incident and problem management RAG matrices.	Operational Delivery Board Pack and separate reports in the event of priority incidents	Monthly or as required in the event of priority incidents
Charges	Breakdown of charges for the period, with reference to the services/products and/or change request/Variation for each charge as appropriate	Template to be agreed with supplier	Monthly
Major sub-contractors	Not applicable unless a major sub-contractor is introduced as part of a Variation to this Agreement. Details to be confirmed at the time.	Not applicable unless a major sub-contractor is introduced as part of a Variation to this Agreement. Details to be confirmed at the time.	Not applicable unless a major sub-contractor is introduced as part of a Variation to this Agreement. Details to be confirmed at the time.
Technical	Utilisation. Product roadmap. Design/solution changes in the period. Certificate expiry dates.	Operational Delivery Board Pack	Monthly
Continuous Improvement Plan	As per Schedule 3 (Continuous Improvement)	Template to be agreed with supplier	Annual

Supply Chain Visibility Joint Schedule 12 (3.1-3.3)	SME MI Reports	MI Reporting Template	Monthly
KPI Transparency Reporting	Quarterly publication of performance against three agreed KPIs. Specific KPIs to be confirmed with supplier.	Template to be agreed with supplier	Quarterly
Social Value	Quarterly updates on Social Value activities as part of Senior Strategic Relationship Management.	Quarterly Performance Review Board Pack	Quarterly

Call-Off Schedule 2 (Staff Transfer)

1. Definitions

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

<p>"Employee Liability"</p>	<p>1 all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:</p> <p>a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;</p>
	<p>b) unfair, wrongful or constructive dismissal compensation;</p>
	<p>c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;</p>
	<p>d) compensation for less favourable treatment of part-time workers or fixed term employees;</p>
	<p>e) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Sub-contractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;</p>
	<p>f) claims whether in tort, contract or statute or otherwise;</p>
	<p>any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;</p>

<p>"Former Supplier"</p>	<p>a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Deliverables (or any part of the Deliverables) and shall include any Sub-contractor of such supplier (or any Sub-contractor of any such Sub-contractor);</p>
<p>"Partial Termination"</p>	<p>the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);</p>
<p>"Relevant Transfer"</p>	<p>a transfer of employment to which the Employment Regulations applies;</p>
<p>"Relevant Transfer Date"</p>	<p>in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate;</p>
<p>"Supplier's Final Supplier Personnel List"</p>	<p>a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date;</p>
<p>"Supplier's Provisional Supplier Personnel List"</p>	<p>a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;</p>

<p>"Staffing Information"</p>	<p>in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format:</p> <p>(a) their ages, dates of commencement of employment or engagement, gender and place of work;</p>
	<p>(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;</p>
	<p>(c) the identity of the employer or relevant contracting Party;</p>
	<p>(d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;</p>
	<p>(e) their wages, salaries, bonuses and profit sharing arrangements as applicable;</p>
	<p>(f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;</p>
	<p>(g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);</p>
	<p>(h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;</p>
	<p>(i) copies of all relevant documents and materials relating to such information, including copies of</p>

	relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and
	(j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;
"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date;
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date.

2. INTERPRETATION

Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be and where the Sub-contractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

3. Which parts of this Schedule apply

Only the following parts of this Schedule shall apply to this Call Off Contract:

- Part C (No Staff Transfer On Start Date)
- Part E (Staff Transfer on Exit)

Part C: No Staff Transfer on the Start Date

1. What happens if there is a staff transfer

- 1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.
- 1.2 Subject to Paragraphs 1.3, 1.4 and 1.5, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then:
- 1.2.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;
 - 1.2.2 the Buyer may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;
 - 1.2.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;
 - 1.2.4 if after the period referred to in Paragraph 1.2.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;
- and subject to the Supplier's compliance with Paragraphs 1.2.1 to 1.2.4:
- (a) the Buyer will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2; and
 - (b) the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Sub-contractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2.
- 1.3 The indemnities in Paragraph 1.2 shall not apply to any claim:
- 1.3.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Sub-contractor; or

- 1.3.2 any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure
 - 1.4 The indemnities in Paragraph 1.2 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.
 - 1.5 If the Supplier and/or the Sub-contractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Sub-contractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.
- 2. Limits on the Former Supplier's obligations**

Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

- 1.1 The Supplier agrees that within 20 Working Days of the earliest of:
- 1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;
 - 1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;
 - 1.1.3 the date which is 12 Months before the end of the Term; and
 - 1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Laws, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

- 1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Sub-contractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).
- 1.3 The Buyer shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Sub-contractor.
- 1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Sub-contractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.
- 1.5 From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall, unless otherwise instructed by the Buyer (acting reasonably):

not replace or re-deploy any Supplier Personnel listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and

expertise and is employed on the same terms and conditions of employment as the person he/she replaces

not make, promise, propose, permit or implement any material changes to the terms and conditions of (i) employment and/or (ii) pensions, retirement and death benefits (including not to make pensionable any category of earnings which were not previously pensionable or reduce the pension contributions payable) of the Supplier Personnel (including any payments connected with the termination of employment);

- 1.5.1 not increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;
- 1.5.2 not introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
- 1.5.3 not increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);
- 1.5.4 not terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;
- 1.5.5 not dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor;
- 1.5.6 give the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor reasonable access to Supplier Personnel and/or their consultation representatives to inform them of the intended transfer and consult any measures envisaged by the Buyer, Replacement Supplier and/or Replacement Sub-contractor in respect of persons expected to be Transferring Supplier Employees;
- 1.5.7 co-operate with the Buyer and the Replacement Supplier to ensure an effective consultation process and smooth transfer in respect of Transferring Supplier Employees in line with good employee relations and the effective continuity of the Services, and to allow for participation in any pension arrangements to be put in place to comply with New Fair Deal;
- 1.5.8 promptly notify the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Sub-contractor of any notice to terminate employment given by the Supplier or received from any persons listed on the Supplier's Provisional

- Supplier Personnel List regardless of when such notice takes effect;
- 1.5.9 not for a period of 12 Months from the Service Transfer Date re-employ or re-engage or entice any employees, suppliers or Sub-contractors whose employment or engagement is transferred to the Buyer and/or the Replacement Supplier (unless otherwise instructed by the Buyer (acting reasonably));
 - 1.5.10 not to adversely affect pension rights accrued by all and any Fair Deal Employees in the period ending on the Service Transfer Date;
 - 1.5.11 fully fund any Broadly Comparable pension schemes set up by the Supplier;
 - 1.5.12 maintain such documents and information as will be reasonably required to manage the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract (including without limitation identification of the Fair Deal Employees);
 - 1.5.13 promptly provide to the Buyer such documents and information mentioned in Paragraph 3.1.1 of Part D: Pensions which the Buyer may reasonably request in advance of the expiry or termination of this Contract; and
 - 1.5.14 fully co-operate (and procure that the trustees of any Broadly Comparable pension scheme shall fully co-operate) with the reasonable requests of the Supplier relating to any administrative tasks necessary to deal with the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract.
- 1.6 On or around each anniversary of the Effective Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide such information as the Buyer may reasonably require which shall include:
- 1.6.1 the numbers of employees engaged in providing the Services;
 - 1.6.2 the percentage of time spent by each employee engaged in providing the Services;
 - 1.6.3 the extent to which each employee qualifies for membership of any of the Fair Deal Schemes (as defined in Part D: Pensions); and
 - 1.6.4 a description of the nature of the work undertaken by each employee by location.

- 1.7 The Supplier shall provide all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Sub-contractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Sub-contractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
- 1.7.1 the most recent month's copy pay slip data;
 - 1.7.2 details of cumulative pay for tax and pension purposes;
 - 1.7.3 details of cumulative tax paid;
 - 1.7.4 tax code;
 - 1.7.5 details of any voluntary deductions from pay; and
 - 1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

- 2.1 A change in the identity of the supplier of the Services (or part of the Services), howsoever arising, may constitute a Relevant Transfer to which the Employment Regulations will apply. The Buyer and the Supplier agree that where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Sub-contractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Fair Deal Schemes (as defined in Part D: Pensions).
- 2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Sub-contractor against any Employee Liabilities arising from or as a result of any act or omission of the Supplier or any Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date.

- 2.4 The indemnity in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Sub-contractor whether occurring or having its origin before, on or after the Service Transfer Date.
- 2.5 Subject to Paragraphs 2.6 and 2.7, if any employee of the Supplier who is not identified in the Supplier's Final Transferring Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Sub-contractor pursuant to the Employment Regulations then.
- 2.5.1 the Replacement Supplier and/or Replacement Sub-contractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing;
 - 2.5.2 the Supplier may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Sub-contractor;
 - 2.5.3 if such offer of employment is accepted, the Replacement Supplier and/or Replacement Sub-contractor shall immediately release the person from its employment;
 - 2.5.4 if after the period referred to in Paragraph 2.5.2 no such offer has been made, or such offer has been made but not accepted, the Replacement Supplier and/or Replacement Sub-contractor may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Replacement Supplier's and/or Replacement Sub-contractor's compliance with Paragraphs 2.5.1 to 2.5.4 the Supplier will indemnify the Replacement Supplier and/or Replacement Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees referred to in Paragraph 2.5.

- 2.6 The indemnity in Paragraph 2.5 shall not apply to:
- 2.6.1 (a) any claim for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief, or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Replacement Supplier and/or Replacement Sub-contractor, or
 - 2.6.2 (b) any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Sub-contractor neglected to follow a fair dismissal procedure.

- 2.7 The indemnity in Paragraph 2.5 shall not apply to any termination of employment occurring later than 3 Months from the Service Transfer Date.
- 2.8 If at any point the Replacement Supplier and/or Replacement Sub-contract accepts the employment of any such person as is described in Paragraph 2.5, such person shall be treated as a Transferring Supplier Employee and Paragraph 2.5 shall cease to apply to such person.
- 2.9 The Supplier shall promptly provide the Buyer and any Replacement Supplier and/or Replacement Sub-contractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Sub-contractor, shall promptly provide to the Supplier and each Sub-contractor in writing such information as is necessary to enable the Supplier and each Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.10 Subject to Paragraph 2.9, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Sub-contractor and its Sub-contractors against any Employee Liabilities arising from or as a result of any act or omission, whether occurring before, on or after the Service Transfer Date, of the Replacement Supplier and/or Replacement Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee.
- 2.11 The indemnity in Paragraph 2.10 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Sub-contractor (as applicable) to comply with its obligations under the Employment Regulations, or to the extent the Employee Liabilities arise out of the termination of employment of any person who is not identified in the Supplier's Final Supplier Personnel List in accordance with Paragraph 2.5 (and subject to the limitations set out in Paragraphs 2.6 and 2.7 above).

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

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

2. Supplier's Obligations

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

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

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

2.3.1 identifying the emergence of relevant new and evolving technologies;

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

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

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

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred

(100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

- 2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.
- 2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
- 2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
- 2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
- 2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
 - 2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
- 2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
- 2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.
- 2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
- 2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 5 (Pricing Details)

[REDACTED]	[REDACTED]																								
[REDACTED]	<table border="1"><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]																						
[REDACTED]	[REDACTED]																								
[REDACTED]	[REDACTED]																								
[REDACTED]	[REDACTED]																								

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Annex 1 to this Schedule 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.

Annex 1- Key Roles

Key Role
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

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

1. Definitions

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

"BCDR Plan"	1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster Recovery Deliverables"	3 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	4 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	5 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	6 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	7 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	8 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

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

2.2 The Buyer recognises that in most cases the Supplier will have in place a BCDR Plan for their services which will meet industry standards and satisfy the Buyer's requirements. Where this is the case this should be provided to the Customer at the earliest opportunity. It is acknowledged that as these form part of a standard service it may not be possible for a Customer to request adjustments to the plan.

- 2.3 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "**BCDR Plan**"), which shall detail the processes and arrangements that the Supplier shall follow to:
- 2.3.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and
 - 2.3.2 the recovery of the Deliverables in the event of a Disaster
- 2.4 The BCDR Plan shall be divided into three sections:
- 2.4.1 Section 1 which shall set out general principles applicable to the BCDR Plan;
 - 2.4.2 Section 2 which shall relate to business continuity (the "**Business Continuity Plan**"); and
 - 2.4.3 Section 3 which shall relate to disaster recovery (the "**Disaster Recovery Plan**").
- 2.5 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

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

- 3.1 Section 1 of the BCDR Plan shall:
- 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
 - 3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
 - 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
 - 3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

- 3.1.6 contain a risk analysis, including:
 - (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
 - (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - (c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
 - (d) a business impact analysis of different anticipated failures or disruptions;
- 3.1.7 provide for documentation of processes, including business processes, and procedures;
- 3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- 3.1.9 identify the procedures for reverting to "normal service";
- 3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
- 3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and
- 3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.
- 3.2 The BCDR Plan shall be designed so as to ensure that:
 - 3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
 - 3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
 - 3.2.4 it details a process for the management of disaster recovery testing.
- 3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
- 3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

- 4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
- 4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
 - 4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.
- 4.2 The Business Continuity Plan shall:
- 4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
 - 4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
 - 4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
 - 4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

- 5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
- 5.2.1 loss of access to the Buyer Premises;
 - 5.2.2 loss of utilities to the Buyer Premises;
 - 5.2.3 loss of the Supplier's helpdesk or CAFM system;
 - 5.2.4 loss of a Subcontractor;
 - 5.2.5 emergency notification and escalation process;
 - 5.2.6 contact lists;
 - 5.2.7 staff training and awareness;

- 5.2.8 BCDR Plan testing;
- 5.2.9 post implementation review process;
- 5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
- 5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
- 5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
- 5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

- 6.1 The Supplier shall review the BCDR Plan:
 - 6.1.1 on a regular basis and as a minimum once every six (6) Months;
 - 6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and
 - 6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.
- 6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
- 6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a "**Review Report**") setting out the Supplier's proposals (the "**Supplier's Proposals**") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

- 7.1 The Supplier shall test the BCDR Plan:
- 7.1.1 regularly and in any event not less than once in every Contract Year;
 - 7.1.2 in the event of any major reconfiguration of the Deliverables
 - 7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
- 7.5.1 the outcome of the test;
 - 7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - 7.5.3 the Supplier's proposals for remedying any such failures.
- 7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

- 8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

- 9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

Not Used

Part B: Long Form Security Requirements

1. Definitions

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

<p>"Breach of Security "</p>	<p>1 means the occurrence on cloud service environments or equipment controlled by Supplier affecting the confidentiality, availability, and integrity of such Buyer confidential information:</p> <ul style="list-style-type: none"> a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, <p>2 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;</p>
<p>"ISMS"</p>	<p>3 the information security management system and process developed by the Supplier on cloud service environments or equipment controlled by Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and</p>
<p>"Security Tests"</p>	<p>4 tests to validate the ISMS and security of all relevant processes, systems, incident response</p>

	plans, patches to vulnerabilities and mitigations to Breaches of Security.
Security Vulnerabilities	5 Given meaning in Call Off Schedule 14 Service Levels

2. Security Requirements

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

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 Don Kavanagh

2.3.2 Alastair Skelton

2.4 The Buyer shall clearly articulate its high-level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day-to-day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall make available to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and

availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

- 3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and
- 3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

- 3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
- 3.4.2 meet the relevant standards in ISO/IEC 27001
- 3.4.3 at all times provide a level of security which:
 - a) is in accordance with the Law and this Contract;
 - b) complies with the Baseline Security Requirements;
 - c) as a minimum demonstrates Good Industry Practice;
 - d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
 - e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)
(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
 - f) takes account of guidance issued by the Centre for Protection of National Infrastructure
(<https://www.cpni.gov.uk>)
 - g) complies with HMG Information Assurance Maturity Model and Assurance Framework
(<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall make available to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan as agreed between the parties which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan, relevant to this agreement shall:

- 4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
- 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
- 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- 4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;
- 4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- 4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);
- 4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available,

appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

- 4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;
- 4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
- 4.2.10 be structured in accordance with ISO/IEC27001, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
- 4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
- 4.2.12 for the avoidance of doubt, not to be considered to include the Supplier's corporate security management plan

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

- 5.1.1 emerging changes in Good Industry Practice;

- 5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
 - 5.1.3 any new perceived or changed security threats;
 - 5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
 - 5.1.5 any new perceived or changed security threats; and
 - 5.1.6 any reasonable change in requirement requested by the Buyer.
- 5.2 The Supplier shall provide, where reasonable and applicable, the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- 5.2.1 suggested improvements to the effectiveness of the ISMS;
 - 5.2.2 updates to the risk assessments;
 - 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
 - 5.2.4 suggested improvements in measuring the effectiveness of controls.
- 5.3 Any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Supplier shall provide the Buyer annually with the results of such Security Tests (in a form approved by the Buyer in advance).
- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests, subject to Suppliers Vulnerability Testing Policy) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability

to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. The Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Security Breach

7.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Supplier shall:

7.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- a) minimise the extent of actual or potential harm caused by any Breach of Security;
- b) remedy such Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
- c) where deemed necessary, apply a tested mitigation against any such Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting

- reasonably, may specify by written notice to the Supplier;
- d) take reasonable steps to prevent a further Breach of Security exploiting the same root cause failure; and
 - e) supply relevant requested data and updates until the matter is remediated to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request without unreasonable delay and without charge (where such requests are reasonably related to an actual incident or compromise); and
 - f) as soon as reasonably practicable provide to the Buyer the summary or full details, where requested, (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

7.3 In the event that any action is taken in response to a Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

8. Security Vulnerabilities and fixing them

8.1 The Buyer and the Supplier acknowledge that from time to time Security Vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

8.2 The severity of threat Security Vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the Security Vulnerability scoring according to the agreed method in the ISMS and using the appropriate Security Vulnerability scoring systems including:

8.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

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

8.3 The Supplier shall procure the application of security patches to Security Vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

8.3.1 the Supplier can demonstrate that a Security Vulnerability is not exploitable within the context of any Service (e.g. because it resides

in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the Security Vulnerability becomes exploitable within the context of the Service;

8.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

8.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

8.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

8.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

8.4.2 is agreed with the Buyer in writing.

8.5 The Supplier shall:

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

8.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

8.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

8.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

8.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the

control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

8.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

8.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

8.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

8.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 8, the Supplier shall immediately notify the Buyer.

8.7 A failure to comply with Paragraph 8.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme (“CPA”).

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks apply to Processor, and subsequently, Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage with the Buyer in accordance with Clause 14 (Data protection) and Joint Schedule 11 (Processing Data).

3.3 The Supplier shall provide a self-service process to allow the Buyer to:

- 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted, by the Supplier, over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device must be subject to protective measures appropriate to the security level of such Government Data, as agreed by the parties, using a product or system component which has been formally assured through a certification process recognised by the Buyer.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff within the UK shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 Supplier Staff outside of the UK shall be subject to pre-employment checks that include, as a minimum: identity and right to work (or equivalent). Supplier Staff will be subject to the Supplier's code of conduct policies.

6.3 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system

administrators with privileged access to IT systems which store or process Government Data.

- 6.4 For Professional Services the Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.5 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- 6.6 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

- 7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain a record of accesses

8. Audit

- 8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
- 8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
 - 8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

1. GDPR

Definitions

The service states that it will comply with ISO standards

- a) complies with ISO/IEC27001

The particular needs for this for an ISO mapping will be as follows. This mapping table does not constitute as legal advice for meeting the European General Data Protection Regulation (EU GDPR) requirements. Upon reviewing the mapping table, please note that the ISO 27001 controls without the prefix 'A' are in the main body of ISO/IEC 27001:2013. Those prefixed with 'A' are listed in Annex A of ISO 27001:2013. a supplementary guideline standard on information security controls.

GDPR V ISO 27001 Mapping Table

This mapping table does not constitute as legal advice for meeting the European General Data Protection Regulation (EU GDPR) requirements. Upon reviewing the mapping table, please note that the ISO 27001 controls without the prefix 'A' are in the main body of ISO/IEC 27001:2013. Those prefixed with 'A' are listed in Annex A of ISO 27001:2013 – a supplementary guideline standard on information security controls.

Under these principles of GDPR to assure from a SOA that the supplier must comply to the following controls. Similarly the Controller (HMRC) should enforce this with Supplier XXXXX as the processor of the Data.

1.1.2 **NOTES 1 processor : Processors are responsible for securing the service Under Article 32 of GDPR. Company XXXXXXX**

- a) A processor may make its own day-to-day operational decisions, but Article 29 says it should only process personal data in line with a controller's instructions, unless it is required to do otherwise by UK law (in that case it must inform the controller of this legal requirement before the processing, unless that law prohibits it doing so on important grounds of public interest). This is also a required contract term under Article 28 (3)(a).

1.2 If a processor acts outside of a controller's instructions in such a way that it decides the purpose and means of processing, then it will be a controller and will have the same liability as a controller.

2. What responsibilities does a processor have in its own right?

2.1 In addition to the contract terms, a processor also has some direct responsibilities and liabilities under the UK GDPR. When drawing up and negotiating a contract for data processing, it is good practice for all parties to make sure they understand this.

2.2 The parties may also wish to explicitly cover this in the contract, although the UK GDPR doesn't require it. For example they may wish to include a clause specifying that nothing in the contract relieves the processor or controller of its own direct responsibilities and liabilities under the UK GDPR – and to say what these are.

2.3 Articles that affect processor are as follows [Relevant provisions in the UK GDPR - See Articles 3, 5, 27, 28, 29, 30, 31, 32, 33.2, 37, 38, 82, 83 and 84 and Recitals 22, 23, 24, 39, 80, 81, 85, 87, 88, 91, 97, 146, 148, 149, 150 and 152](#)

3. Notes 2: responsibility of the controller (HMRC)

3.1 The controller is responsible for assessing that its processor is competent to process personal data in line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects. This is because Article 28(1) says a controller must only use a processor that can provide "sufficient guarantees" (in particular in terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals.

3.2 Some examples of the consideration's controllers should have when assessing whether the processor provides "sufficient guarantees" could include:

- the extent to which they comply with industry standards, if these apply in the context of the processing;
- whether they have sufficient technical expertise to assist the controller, eg in carrying out obligations under Articles 32-36 of the UK GDPR (technical measures, breach notifications and DPIAs);
- providing the controller with relevant documentation, eg their privacy policy, record management policy and information security policy; and
- adherence to an approved code of conduct or a certification scheme (when they become available).

3.3 This is not an exhaustive list, and ultimately it is for the controller to satisfy itself that the processor provides sufficient guarantees in the context of the processing. Whether the guarantees are sufficient will depend on both the circumstances of the processing and the risk posed to rights of individuals.

- 3.4 Once the controller has chosen a suitable processor, it must put in place a contract or other legal act that meets all the requirements of Article 28(3) and give the processor documented instructions to follow (either in the contract or separately).
- 3.5 However, the controller's responsibilities do not end there. Controllers should ensure a processor's compliance on an ongoing basis, in order for them to satisfy the accountability principle and demonstrate due diligence. In particular, Article 28(3)(h) explicitly requires the processor to allow for and contribute to audits and inspections, carried out either by the controller or a third party appointed by the controller. The methods used to monitor compliance and the frequency of monitoring will depend on the circumstances of the processing.
4. What is a controller's liability when it uses a processor?
- 4.1 A controller is primarily responsible for its own compliance and ensuring the compliance of its processors. This means that, regardless of the terms of the contract with a processor, the controller may be subject to any of the corrective measures and sanctions set out in the UK GDPR. These include orders to bring processing into compliance, claims for compensation from a data subject and administrative fines. For more details about how we exercise our powers, please see the [taking action](#) page on our website.
- 4.2 An individual can bring claims directly against a controller if the processing breaches the UK GDPR, in particular where the processing causes the individual damage.
- 4.3 A controller will be liable for any damage (and any associated claim for compensation payable to an individual) if its processing activities infringe the UK GDPR.
- 4.4 However, a controller will not be liable for damage resulting from a breach of the UK GDPR if it can prove it was not in any way responsible for the event giving rise to the damage.

If a processor is involved in the processing, the individual making the claim for compensation can claim against either party. If a controller has to pay full compensation for damage suffered by individuals, it may be able to claim back all or part of the amount of compensation from a processor involved in the processing, to the extent that the processor is at fault. Penalty regime must be in line with GDPR regulations. The SLA (service level agreement) may apply further punitive charges depending on SLA, Breach Notification

GDPR articles that affect the controller in addition are as follows

5. This mapping table compliance

This mapping table does not constitute as legal advice for meeting the European General Data Protection Regulation (EU GDPR) requirements. Upon reviewing the mapping table, please note that the ISO 27001 controls without the prefix 'A' are in the main body of ISO/IEC 27001:2013. Those prefixed with 'A' are listed in Annex A of ISO 27001:2013 – a supplementary guideline standard on information security controls.

Under these principles of GDPR to assure from a SOA that the supplier must comply to the following controls. Similarly, the Controller (HMRC) should enforce this with Supplier XXXXX as the processor of the Data.

GDPR		ISO 27001	
Article	Outline/Summary	Control	Notes
<i>Chapter I – General Provisions</i>			

<p>1 – Subject matter & Objectives</p>	<p>GDPR concerns the protection and free movement of “personal data”, defined in article 4 as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.</p>	<p>A.18.1.4</p>	<p>The ISO 27001 standards concern information risks, particularly the management of information security controls mitigating unacceptable risks to organisations’ information. In the context of GDPR, privacy is largely a matter of securing people’s personal information, particularly sensitive computer data. The ISO 27001 standards specifically mention compliance obligations relating to the privacy and protection of personal info (more formally known as Personally Identifiable Information - PII - in some countries) in control A.18.1.4.</p>
<p>2 – Material Scope</p>	<p>GDPR concerns “the processing of personal data wholly or partly by automated means” (Essentially, IT systems, apps and networks) and in a business or corporate/organisational context (private home uses are not in scope).</p>	<p>Many</p>	<p>ISO 27001 concerns information in general, not just computer data, systems, apps and networks. It is a broad framework, built around a ‘management system’. ISO 27001 systematically addresses information risks and controls throughout the organisation as a whole, including but going beyond the privacy and compliance aspects.</p>
<p>3 – Territorial Scope</p>	<p>GDPR concerns personal data for people in the European Union whether is it processed in the EU or elsewhere</p>	<p>A.18.1.4, etc.</p>	<p>ISO 27001 is global in scope. Any organisation that interacts with people in the European Union may fall under GDPR, especially of course if they collect personal info.</p>
<p>4 – Definitions</p>	<p>GDPR privacy-related terms are formally defined here.</p>	<p>3</p>	<p>ISO/IEC 27000 defines most ISO 27001 terms including some privacy terms. Many organisations have their own glossaries in this area. Check that any corporate definitions do not conflict with GDPR.</p>

Chapter II - Principles			
<p>5 – Principles relating to processing of personal data</p>	<p>Personal data must be: (a) processed lawfully, fairly and transparently; (b) collected for specified, explicit and legitimate purposes only; (c) adequate, relevant and limited; (d) accurate; (e) kept no longer than needed; (f) processed securely to ensure its integrity and confidentiality</p>	<p>6.1.2, A.8.1.1, A.8.2, A. 8.3, A.9.1.1, A.9.4.1, A.10, A. 13.2, A.14.1.1, A.15, A.17, A.18 ... in fact almost all!</p>	<p>Business processes plus apps, systems and networks must adequately secure personal information, requiring a comprehensive suite of technological, procedural, physical and other controls ... starting with an assessment of the associated information risks. See also 'privacy by design' and 'privacy by default' (Article 25). In order to satisfy these requirements, organisations need to know where personal info is, classify it and apply appropriate measures to address (a)-(f).</p>
<p>6 – Lawfulness of processing</p>	<p>Lawful processing must: (a) be consented to by the subject for the stated purpose; (b) be required by a contract; (c) be necessary for other compliance reasons; (d) be necessary to protect someone's vital interests; (e) be required for public interest or an official authority; and/or (f) be limited if the subject is a child.</p>	<p>6.1.2, A.14.1.1, A.18.1.1 etc.</p>	<p>This should also be covered in the assessment and treatment of information risks. It will influence the design of business processes/activities, apps, systems etc. (e.g. it may be necessary to determine someone's age before proceeding to collect and use their personal info). These are business requirements to limit and protect personal information: many security controls are required in practice to mitigate unacceptable information risks that cannot be avoided (by not collecting/using the data) or shared (e.g. relying on some other party to get consent and collect the data - a risk in its own right!).</p>

7 – Conditions for consent	The data subject’s consent must be informed, freely given and they can withdraw it easily at any time.	A.8.2.3, A.12.1.1, A.13.2.4, A.18.1.3, 6.1.2, A.14.1.1, A.8.3.2, A.13.2, etc.	There is a requirement to request informed consent for processing (otherwise stop!) and to be able to demonstrate this. Procedures need to be in place for this and records demonstrating the consent must be protected and retained. Withdrawal of consent implies the capability to locate and remove the personal info, perhaps during its processing and maybe also from backups and archives, plus business processes to check and handle requests
8 – Conditions applicable to child’s consent in relation to information society services	Special restrictions apply to consent by/for children.	See Article 7	These special restrictions apply primarily at the time information is gathered (e.g. getting a parent’s consent).
9 – Processing of special categories of personal data	Special restrictions apply to particularly sensitive data concerning a person’s race, political opinions, religion, sexuality, genetic info and other biometrics etc. Processing of such info is prohibited by default unless consent is given and processing is necessary (as defined in the Article).	A.8.2.1, A.8.2.3, A.14.1.1	See 7 above. It is important to identify where sensitive data may be processed, whether that is ‘necessary’ in fact, and to obtain explicit consent - factors to be considered in the design of systems, apps and business processes.
10 – Processing of personal data relating to criminal convictions and offences	Special restrictions also apply to personal data concerning criminal convictions and offences.	A. 7.1, A.8.2.1, A.8.2.3, 6.1.2, A.14.1.1, A.7.1, etc.	Any use of this information should be identified and only processed in specific circumstances. Such information should preferably not be retained except by the authorities ... but may be needed for background checks, credit/fraud risk profiling etc.

11 – Processing which does not require identification	Some restrictions don't apply if a person cannot be identified from the data held.	A.8.2.1, A.8.2.3, 6.1.2, A.14.1.1, etc.	Avoiding information risks (by NOT knowing who the subjects are) is a good option, where feasible: does the business really need to know a person's identity or will aggregate info/statistics suffice?
Chapter III – Rights of the Data Subject			
Section 1 – Transparency & modalities			
12 – Transparent notifications, processes. It may also communication & A.16 relation to their own responding promptly,	Communications with data subjects must be information, transparent, clear and easily be relevant to etc. incident management i.e. mechanisms personal information (implying a means and for the data subject keeping records of	A.12.1.1 allowing exercise such	See above. This affects the wording of web forms, understood. A.14.1.1 telephone scripts etc. plus the people to enquire or modalities for the complain in of the rights of to identify and authenticate them), for communications (e.g. to limit or charge for excessive requests)
Section 2 – Information and access to personal information			
13 – Information to be provided where personal data are collected from the data subject	When personal data are collected, people must be given (or already possess) several specific items of information such as details of the data controller” and “data protection officer”, whether their info will be exported (especially outside the EU), how long the info will be held, their rights and how to enquire/complain etc.	A.8.2., A.8.2.3, A.12.1.1, A.14.1.1, A.16, etc.	Procedures for the provision of fair processing information, information on the data controller and purposes for processing the data need to be defined and implemented. This relies in part on identifying where personal info is in use.
14 – Information to be provided where personal data have not been obtained from the data subject	Similar notification requirements to Article 13 apply if personal info is obtained indirectly (e.g. a commercial mailing list?): people must be informed within a month and on the first communication with them.	A.8.2.1, A.8.2.3, A.12.1.1, A.14.1, A.16, etc.	See Article 13

15 – Right of access by the data subject	People have the right to find out whether the organisation holds their personal info, what it is being used for, to whom it may be disclosed etc., and be informed of the right to complain, get it corrected, insist on it being erased etc. People have rights to obtain a copy of their personal information	A.8.1.1, A.8.2.1, A.12.1.1, A.13.2.1, A.14.1.1, etc.	Subject rights include being able to obtain a copy of their own info (again implying the need for identification and authentication before acting on such requests), disclosing the nature of processing e.g. the logic behind and the consequences of ‘profiling’, and info about the controls if their data are exported. It may also affect backup and archive copies. See also Article 7 on withdrawal of consent.
Section 3 – Rectification & Erasure			
16 – Right to rectification	People have the right to get their personal info corrected, completed, clarified etc.	A.12.1.1, A.14.1, A.9, A.16, A.12.3, A.18.1.3	Implies functional requirements to check, edit and extend stored info, with various controls concerning identification, authentication, access, validation etc. It may also affect backup and archive copies.
17 – Right to erasure ('Right to be forgotten')	People have a right to be forgotten i.e. to have their personal info erased and no longer used.	6.1.2, A.14.1.1, A.9, A.16, A.12.3, A.8.3.2	This is a form of withdrawing consent (see Article 7). Implies system & process functional requirements to be able to erase specific stored info, with various controls concerning identification, authentication, access, validation etc. It may also affect backup and archive copies.
18 – Right to restriction of processing	People have a right to restrict processing of their personal info	6.1.2, A.8.2.1, A.8.2.3, A.12.1.1, A.14.1.1, A.16, A.12.3, A.18.1.1	See Articles 7, 12 etc. May need ways to identify the specific data that is to be restricted and implement new handling / processing rules. Note it may also affect backup and archive copies.

19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing	People have a right to know the outcome of requests to have their personal info corrected, completed, erased, restricted etc.	A.12.1.1, 6.1.2, A.14.1.1, A.16 etc.	Informing/updating the originator is a conventional part of the incident management process, but there may be a separate or parallel process specifically for privacy complaints, requests etc. since the originators here are not usually employees/insiders.
20 – Right to Data Portability	People have a right to obtain a usable 'portable' electronic copy of their personal data to pass to a different controller.	6.1.2, A.13, A.14.1.1, A.8.3, A.10, A.18.1.3 etc.	Depending on your organisation's purpose, this may seem such an unlikely scenario in practice (low risk) that it may best be handled by exception, manually, without automated IT system functions. Note that the extracted data must be limited to the identified and authenticated person/s concerned, and must be communicated securely, probably encrypted. It may also imply erasing or restricting the data and confirming this (Articles 17, 18 and 19).
Section 4 – Right to object and automated individual decision-making			
21 – Right to object	People have a right to object to their information being used for profiling and marketing purposes	6.1.2, A.12.1.1, A.14.1.1, A.16, A.12.3, etc.	See article 18. May need ways to identify the specific data that is not to be processed and implement new handling / processing rules.
22 – Automated individual decisionmaking	People have a right to insist that key decisions arising from automatic processing of their personal info are manually reviewed/reconsidered	6.1.2, A.12.1.1, A.14.1.1, A.16	Profiling and decision support systems involving personal info must allow manual review and overrides, with the appropriate authorization, access and integrity controls etc.

Section 5 - Restrictions			
23 – Restrictions	National laws may modify or override various rights and restrictions for national security and other purposes.	A.18.1.1	This is primarily of concern to the authorities/public bodies and their systems (e.g. police, customs, immigration, armed forces), but may affect some private/commercial organisations, either routinely (e.g. legal sector, defence industry, ISPs, CSPs, money laundering rules in financial services?) or by exception (implying a legally-sound manual process to assess and handle such exceptional situations).
Chapter IV – Controller & Processor			
Section 1 – General Obligations			
24 – Responsibility of the controller	The “controller” (generally the organisation that owns and benefits from processing of personal info) is responsible for implementing appropriate privacy controls (including policies and codes of conduct) considering the risks, rights and other requirements within and perhaps beyond GDPR.	4, 5, 6, 7, 8, 9, 10 and much of Annex A	This is a formal reminder that a suitable, comprehensive mesh of privacy controls must be implemented, including policies and procedures as well as technical, physical and other controls addressing the information risks and compliance obligations. The scale of this typically requires a structured, systematic approach to privacy. Given the overlaps, it normally makes sense to integrate or at least align and coordinate privacy with the ISO 27001 ISMS and other aspects such as compliance and business continuity management - in other words, it is a governance issue.

<p>25 – Data protection by design and by default</p>	<p>Taking account of risks, costs and benefits, there should be adequate protection for personal info by design, and by default.</p>	<p>6 and much of Annex A</p>	<p>There are business reasons for investing appropriately in privacy, including information risks and compliance imperatives, as well as implementation options with various costs and benefits: elaborating on these is a good way to secure management support and involvement, plus allocate the funding and resources necessary to design, deliver, implement and maintain the privacy arrangements. Privacy by design and by default are examples of privacy principles underpinning the specification, design, development, operation and maintenance of privacy-related IT systems and processes, including relationships and contracts with third parties e.g. ISPs and CSPs</p>
<p>26 – Joint Controllers</p>	<p>Where organisations are jointly responsible for determining and fulfilling privacy requirements collaboratively, they must clarify and fulfil their respective roles and responsibilities.</p>	<p>5.3 9.1 A.13.2 A.15 A.16 A.18.1</p>	<p>Organisations need to manage relationships with business partners, ensuring that privacy and other information security aspects don't fall between the cracks. This includes, for instance, jointly investigating and resolving privacy incidents, breaches or access requests, achieving and maintaining an assured level of GDPR compliance and respecting consented purposes for which personal info was initially gathered, regardless of where it ends up.</p>
<p>27 – Representatives of controllers or processors not established in the Union</p>	<p>Organisations outside Europe must formally nominate privacy representatives inside Europe if they meet certain conditions (e.g. they routinely supply goods and services to, or monitor, Europeans).</p>	<p>5.3, 7.5.1, A.15, A.18.1.4</p>	<p>This is one of many compliance formalities: the Privacy Officer (or Data Protection Officer or equivalent) should be accountable for making sure this is done correctly.</p>

28 – Processor	If an organisation uses one or more third parties to process personal info ('processors'), it must ensure they too are compliant with GDPR.	8.2, 9.1, A.15, A.18.1.1, A.18.1.3, A.18.1.4	This applies to ISPs and CSPs, outsourced data centres etc., plus other commercial services where the organisation passes personal info to third parties e.g. for marketing plus HR, payroll, tax, pension and medical services for employees. It also applies on the receiving end: service suppliers can expect to be questioned about their GDPR compliance status, privacy policies and other controls (e.g. any subcontractors), and to have compliance and assurance clauses/terms and liabilities included in contracts and agreements. The information risks need to be identified, assessed and treated in the normal manner, on both sides.
29 – Processing under the authority of the controller or processing	Processors must only process personal info in accordance with instructions from the controller and applicable laws.	Most	Processors need to secure and control personal info in much the same way as controllers. They may well be controllers for personal info on employees etc. so will hopefully have all necessary privacy arrangements in hand anyway: it's 'just' a case of extending them to cover client info, and manage privacy within client relationships (e.g. how to handle breaches or other enquiries, incidents and issues).
30 – Records of processing activities	Controllers must maintain documentation concerning privacy e.g. the purposes for which personal info is gathered and processed, 'categories' of data subjects and personal data etc.	7.5	Documented information
31 – Cooperation with the supervisory authority	Organisations must cooperate with the authorities e.g. privacy or data protection ombudsmen.	A.6.1.3	Contact with authorities
Section 2 - Security of personal data			

<p>32 – Security of processing</p>	<p>Organisations must implement, operate and maintain appropriate technical and organisational security measures for personal info, addressing the information risks</p>	<p>8.2, 8.3 and most of Annex A</p>	<p>GDPR mentions a few control examples (such as encryption, anonymization and resilience) covering data confidentiality, integrity and availability aspects, plus testing/assurance measures and compliance by workers (implying policies and procedures, awareness/training and compliance enforcement/reinforcement). An ISO 27001 ISMS provides a coherent, comprehensive and structured framework to manage privacy alongside other information risk and security controls, compliance etc.</p>
<p>33 – Notification of a personal data breach to the supervisory authority</p>	<p>Privacy breaches that have exposed or harmed personal info must be notified to the authorities promptly (within 3 days of becoming aware of them unless delays are justified).</p>	<p>A.16, A.18.1.4</p>	<p>Breaches etc. would normally be handled as incidents within the ISMS incident management process but GDPR-specific obligations (such as the 3-day deadline for notifying the authorities) must be fulfilled. Note that the point the clock starts ticking is not explicitly defined: it is arguably appropriate to gather and assess the available information/evident first to determine whether or not a reportable incident has actually occurred i.e. the clock may not start until the incident is declared genuine, not a false-alarm.</p>
<p>34 – Communication of a personal data breach to the data subject</p>	<p>Privacy breaches that have exposed or harmed personal info and hence are likely to harm their interests must be notified to the people so affected 'without undue delay'.</p>	<p>A.16, A.18.1.4</p>	<p>Aside from the legal and ethical considerations and direction/guidance from the privacy authorities, there are obviously significant business issues here concerning the timing and nature of disclosure. This would normally be a part of the incident management process for serious or significant incidents, involving senior management as well as specialists and advisors. Avoiding exactly this situation and the associated business costs, disruption and aggravation is one of the strongest arguments to make privacy a corporate</p>

		<p>imperative, and to invest appropriately in appropriate preventive measures. The same point applies to other serious/significant information incidents of course.</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Section 3 – Data protection impact assessment & prior consultation

<p>35 – Data protection impact assessment</p>	<p>Privacy risks including potential impacts must be assessed, particularly where new technologies/systems/arrangements are being considered, or otherwise where risks may be significant (e.g. ‘profiling’ defined in Article 4 as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”). ‘Significantly risky situations’ are to be defined by the national privacy authorities, apparently</p>	<p>6.1.2, A.6.1.3, A.8.2.1</p>	<p>Again, there are sound business and ethical reasons to identify, assess and treat information risks (including privacy and compliance risks), aside from the GDPR obligations. Privacy-related risks should probably be included in corporate risk registers alongside various other risks. GDPR also hints at integrating the assessment of privacy risks as part of the routine risk assessment activities for business change projects, new IT systems developments etc.</p>
-----------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

36 – Prior Consultation	Privacy risks assessed as “high” [undefined] should be notified to the authorities, giving them the chance to comment.	6.1.2, A.6.1.3, A.8.2.1	The GDPR requirement is well-meaning but vague: this might be covered in corporate policies concerning the precise definition of “high” privacy risks ... but on the other hand explicit inputs from the authorities may be helpful in terms of an official position on the suitability and adequacy of proposed controls - in other words this comes down to a business risk/strategic decision by management.
Section 4 – Data Protection Officer			
37 – Designation of the data protection officer	A data protection officer must be formally identified under specified circumstances e.g. public bodies, organisations regularly and systematically monitoring people on a large scale, or those performing large-scale processing of sensitive personal info relating to criminal records.	5.3, A.6.1.1, A.18.1.4	Aside from GDPR obligation, the “Privacy Officer” role (or equivalent titles) is much more broadly applicable and valuable, whether full or parttime, formal or informal, notifiable or not. There are clearly many angles to privacy: a designated corporate focal point for privacy (ideally a competent privacy specialist or expert) makes sense for virtually all organisations. This is another governance issue.
38 – Position of the data protection officer	[If formally designated] the data protection officer must be supported by the organisation and engaged in privacy matters.	5.3, A.6.1.1, A.18.1.4	See above. Formalities aside, without management support and engagement with the organisation, a Privacy Officer is powerless and pointless.
39 – Tasks of the data protection officer	[If formally designated] the data protection officer must offer advice on privacy matters, monitor compliance, liaise with the authorities, act as a contact point, address privacy risks etc.	5.3, A.6.1.1, A.18.1.4	See above. The GDPR requirements would form the basis of a Privacy Officer role description.
Section 5 – Code of Conduct and certification			

40 – Codes of conduct	Various authorities, associations and industry bodies are anticipated to draw up codes of conduct elaborating on GDPR and privacy, offer them to be formally approved (by an unspecified mechanism) and (where appropriate) to implement their own (member) compliance mechanisms.	5.3, A.6.1.1, A.18.1.4	Although this is a valiant attempt to add weight to industry codes, it struggles to achieve a full legal mandate ... but the ethical obligation is clear: privacy is more than just a matter of strict compliance with formal, legal obligations. Aside from that, codes (and ISO 27001 standards!) offer good practice guidance, and compliance may generate commercial/marketing advantages.
41 – Monitoring of approved codes of conduct	The bodies behind codes of conduct are required to monitor compliance (by their members), independently and without prejudice to the legal and regulatory compliance monitoring conducted by the national authorities.	5.3, A.6.1.1, A.18.1.4	As above
42 – Certification	Voluntary data protection certification schemes offering compliance seals and marks (valid for 3 years) are to be developed and registered.	5.3, A.6.1.1, A.18.1.4	Similar schemes already exist: GDPR gives them some official recognition, on top of the commercial advantages they already exploit.
43 – Certification bodies	Certification bodies that award compliance seals and marks should be competent and accredited for this purpose. The European Commission may impose technical standards for certification schemes.	5.3, A.6.1.1, A.18.1.4	This should improve the credibility and meaning of privacy seals and marks. Since they are voluntary, whether or not to be certified, and which schemes to join, are commercial/business matters for management.
Chapter V – Transfer of personal data to third party countries or international organisations			
44 – General principle for transfers	International transfers and processing of personal info must fulfil requirements laid down in subsequent Articles.	-	preamble

45 – Transfers of the basis of an adequacy decision	Data transfers to countries whose privacy arrangements (laws, regulations, official compliance mechanisms ...) are deemed adequate by the European Commission (i.e. compliant with GDPR) do not require official authorisation or specific additional safeguards.	A.18.1.4	Most formalities are to be handled by the Commission. Compliance involves avoiding transfers to other countries, monitoring the official lists for changes, and ensuring that suitable contracts/agreements and other privacy controls are in place as with other third party data transfers (see Article 28 especially).
46 – Transfers subject to appropriate safeguards	Data transfers to countries whose privacy arrangements (laws, regulations, official compliance mechanisms ...) are not deemed adequate by the European Commission (i.e. compliant with GDPR) but meet certain other criteria require additional safeguards.	A.18.1.4	Essentially, the organisation must implement and ensure the adequacy of privacy controls before transferring personal data to such countries, and subsequently e.g. suitable contractual clauses and compliance activities.
47 – Binding corporate rules	National authorities may approve legally-binding privacy rules permitting transfers to non-approved countries.	A.18.1.4	Formalities may affect contractual terms, compliance arrangements, liabilities etc.
48 – Transfers or disclosure not authorised by Union law	Requirements on European organisations from authorities outside Europe to disclose personal data may be invalid unless covered by international agreements or treaties.	A.18.1.4, A.16	Such situations would normally be handled by legal and regulatory compliance specialists - but may start out as incidents.
49 – Derogations for specific situations	Yet more conditions apply to personal info transfers to non-approved countries e.g. explicit consent by the data subjects	A.18.1.4	The Commission is deliberately making it difficult, or rather taking great care since the privacy risks are higher.
50 – International cooperation for the protection of personal data	International authorities will cooperate on data privacy	N/A	N/A
Chapter VI – Independent supervisory authorities			
Section 1 – Independent status			

51 – 54	Concern national bodies overseeing data privacy	N/A	N/A
Section 2 – Competence, tasks and powers			
55 – 59	Concern national bodies overseeing data privacy	N/A	N/A
Chapter VII – Cooperation & consistency			
Section 1 - Cooperation			
60 – 62	Concern supervisory authorities and the EU Data Protection Board	N/A	N/A
Section 2 - Consistency			
63 – 67	Concern supervisory authorities and the EU Data Protection Board	N/A	N/A
Section 3 – European Data Protection Board			
68 – 76	Concern supervisory authorities and the EU Data Protection Board	N/A	N/A
Chapter VIII – Remedies, liabilities and penalties			
77 – 81	Supervisory authorities can deal with privacy complaints	N/A	N/A
82 – Right to compensation and liability	Anyone damaged by infringements of GDPR has a right to compensation from the controller/s or processor/s	A.18.1.4	Privacy and protection of personally identifiable information

83 – General conditions for imposing administrative fines	Administrative fines imposed by supervisory authorities shall be “effective, proportionate and dissuasive”. Various criteria are defined. Depending on the infringements and circumstances, fines may reach 20 million Euros or up to 4% of total worldwide annual turnover for the previous year if greater	6, A.18.1.4	Such huge fines are clearly intended to be a strong deterrent, representing a significant part of the potential impact of privacy breaches etc. in the organisation’s assessment of GDPR compliance and other privacy risks.
84 – Penalties	Other penalties may be imposed. They too must be “effective, proportionate and dissuasive”.	6, A.18.1.4	As above
Chapter IX – Provisions relating to specific processing situations			
85 – Processing and freedom of expression and information	Countries must balance privacy/data protection rights against freedom of expression, journalism, academic research etc. through suitable laws	6, A.18.1.1, A.18.1.4	Issues under this Article may come down to differing legal interpretations in court, hence again there are information risks to be identified, assessed and treated where personal information is involved.
86 – Processing and public access to official documents	Personal data in official documents may be disclosed if the documents are formally required to be disclosed under ‘freedom of information’-type laws.	6, A.18.1.1, A.18.1.4	It may be feasible to redact personal or other sensitive information instead
87 – Processing of the national identification number	Countries may impose further privacy controls for national ID numbers.	6, A.18.1.1, A.18.1.4	National ID numbers may be used as secret personal authenticators, in which case they must remain confidential to reduce the risk of identity theft. In effect they are sensitive personal information, implying the need for encryption and other security/privacy controls
88 – Processing in the context of employment	Countries may impose further constraints on corporate processing and use of personal information about employees e.g. to safeguard human dignity and fundamental rights.	6, A.18.1.1, A.18.1.4	Employment laws may intersect with GDPR and privacy, further complicating compliance and altering the information risks in this area.

89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	Where personal data are to be archived e.g. for research and statistical purposes, the privacy risks should be addressed through suitable controls such as pseudonymization and data minimization where feasible.	6, A.18.1.4	Privacy concerns remain as long as the data subjects are alive (perhaps longer if their families or communities may be impacted by breaches). Taking account of this, the information risks should be identified, assessed and treated appropriately in the normal way.
90 – Obligations of secrecy	Countries may enact additional laws concerning workers’ secrecy and privacy obligations.	6, A.18.1.1, A.18.1.4	Employment or secrecy laws may intersect with GDPR and privacy, still further complicating compliance and altering the information risks in this area.
91 – Existing data protection rules of churches and religious associations	Pre-existing privacy rules for churches and religious associations may continue, “provided they are brought into line with” GDPR.	A.18.1.4	Privacy and protection of personally identifiable information
Chapter X – Delegated acts and implementing acts			
92 – 99	Concern how GDPR is being enacted by the EU	A.18.1.1	Not relevant to an individual organisation’s privacy arrangements, except in as much as they need to comply with applicable laws and regulations.

Who does Part 3 apply to?- HMRC are a competent authority such that the right to be forgotten may not apply as Citizens have to comply TAX, Customs and excise legislation [Commissioners for Revenue and Customs Act 2005](#) (Please seek advice from HMRC oDPO office (who liaise with <https://ico.org.uk/>) the ICO(Information commissioner’s office)

List of current legal competent bodies

- Financial Conduct Authority
- Legal Services Board
- Civil Aviation Authority
- Gambling Commission
- Office of Gas and Electricity Markets (OfGem)
- Office of Communications (OfCom)
- Lead Enforcement Authority for the purposes of the Estate Agents Act 1979 (1)
- Chartered Trading Standards Institute (on behalf of the Secretary of State for Business, Energy and Industrial Strategy)

HMRC Operates under a Competent authority under the following regulations.

<https://www.gov.uk/government/publications/hmrc-appropriate-policy-document/hmrc-appropriate-policy-document>

6. HMRC is a statutory body with statutory functions and a statutory duty of confidentiality which are set out in the [Commissioners for Revenue and Customs Act 2005](#). As part of HMRC's statutory and corporate functions, we (HMRC) process special category and criminal offence data under:

- Article 6(a) of the UK GDPR (the data subject has given consent to the processing of his or her personal data for one or more specific purposes)
- Article 6(b) of the UK GDPR (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract)
- Article 6(c) of the UK GDPR (processing is necessary for compliance with a legal obligation to which HMRC is subject)
- Article 6(e) of the UK GDPR (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in HMRC)

7. HMRC processes sensitive data when it is necessary for law enforcement purposes under section 35 of the DPA 2018.

8. The [HMRC Privacy Notice](#) has more information about HMRC's data protection policy and procedures, including the kind of information we hold and what it is used for.

Please note this will be article 14 notices, Clearly must be available in any communications with Citizen in any medium including webchat, CRM, any technology and/or paper documentation the Notice must be explicitly visible and available to all that use and are the subject of HMRC systems. In this definition(S) HMRC will be a Competent Authority.

9. Part 3 only applies to competent authorities processing for law enforcement purposes. So, it applies, but is not limited, to:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

10. The appropriate regime is based on the law that applies to the controller. So if you are a processor carrying out a law enforcement function on behalf of a competent authority, you will also be processing under this law enforcement processing regime.

11. Any processing carried out by a competent authority which is not for the **primary purpose** of law enforcement will be covered by the general processing regime under the UK GDPR (read with Part 2 of the DPA 2018).

12. If you are a competent authority, it is very likely that you are also processing personal data under the general processing regime. For example, this may include internal HR processes and procedures, as that processing isn't strictly for law enforcement purposes.

13. Identifying the correct regime is important as there are many key differences between the general processing regime and Part 3 of the DPA 2018, including differences on individuals' rights, lawful basis for processing and governance.

What is a 'competent authority'?

14. A competent authority means:

- a person specified in Schedule 7 of the DPA 2018; or
- any other person if, and to the extent that, they have statutory functions to exercise public authority or public powers for the law enforcement purposes.

15. You need to check whether you are listed as a competent authority (CA) in [Schedule 7 of the DPA 2018](#).

16. If you are not listed in Schedule 7, you may still be a competent authority if you have a legal power to process personal data for law enforcement purposes. For example, local authorities who prosecute trading standards offences or the Environment Agency when prosecuting environmental offences.

Are we processing for law enforcement purposes?

17. If you are a competent authority, when you are deciding which regime applies, the key thing to consider is your **primary purpose** for the processing. This should help you identify whether the processing falls under the UK GDPR rules, or satisfies the criteria of the law enforcement purposes under Part 3 of the DPA 2018.

18. The law enforcement purposes are defined under section 31 of the DPA 2018 as:

19. 'The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

20. So if you are a competent authority processing for one of those purposes, you should comply with the law enforcement processing regime.

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

"Exclusive Assets"	1 Supplier Assets used exclusively by the Supplier or a Key Subcontractor in the provision of the Deliverables;
"Exit Information"	2 has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	3 the person appointed by each Party to manage their respective obligations under this Schedule;
"Net Book Value"	4 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"	5 those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes;
"Registers"	6 the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	7 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"	8 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"	9 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"	10 has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	11 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"	12 Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	13 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"	14 has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	15 has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for contract exit

2.1 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.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

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

("Registers").

2.3 The Supplier shall:

- 2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
 - 2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.
- 2.4 Each Party shall appoint an Exit Manager within three (3) Months of the 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.

3. Assisting re-competition for Deliverables

- 3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").
- 3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
- 3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
- 3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

- 4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer 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.
- 4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan

within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

- 4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;
- 4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;
- 4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;
- 4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
- 4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
- 4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
- 4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
- 4.3.8 proposals for the disposal of any redundant Deliverables and materials;
- 4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
- 4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

- 4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:
 - (a) every six (6) months throughout the Contract Period; and
 - (b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
 - (c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;
 - (d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables

(including all changes under the Variation Procedure);
and

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

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

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

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

- 6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
 - 6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
 - 6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - 6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
 - 6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
- 6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
- 6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

- 7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.
- 7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
 - 7.2.1 vacate any Buyer Premises;
 - 7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;
 - 7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:
 - (a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

- (b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

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

- 8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
- 8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

- 8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");
- 8.2.2 which, if any, of:
 - (a) the Exclusive Assets that are not Transferable Assets; and
 - (b) the Non-Exclusive Assets,the Buyer and/or the Replacement Supplier requires the continued use of; and

- 8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "**Transferring Contracts**"),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the

Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

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

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

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

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

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

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

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

Call-Off Schedule 14 (Service Levels)

1. Definitions

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

<p>"Critical Service Level Failure"</p>	<p>[REDACTED]</p>
<p>"Service Credits"</p>	<p>1 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;</p>
<p>"Service Credit Cap"</p>	<p>2 [REDACTED]</p>
<p>"Service/KPI Level Failure"</p>	<p>3 means a failure to meet the Service Level Performance Measure in respect of a Service Level;</p>
<p>"Service/KPI Level Performance Measure"</p>	<p>4 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and</p>
<p>"Service Level Threshold"</p>	<p>5 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.</p>

2. What happens if you don't meet the Service Levels

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service/KPI Level Performance Measure for each Service Level.
- 2.2 The Supplier acknowledges that any Service/KPI 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/KPI Level Performance Measure.
- 2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.
- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service/KPI Level Failure except where:
- 2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
 - 2.4.2 the Service/KPI Level Failure:

- (a) exceeds the relevant Service Level Threshold;
 - (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;
 - (c) results in the corruption or loss of any Government Data; and/or
 - (d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or
- 2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).
- 2.5 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/KPI Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:
- 2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;
 - 2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and
 - 2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.2 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:

- 1.1 is likely to or fails to meet any Service/KPI Level Performance Measure; or
- 1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

- 1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service/KPI Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.2.2 instruct the Supplier to comply with the Rectification Plan Process;
- 1.2.3 if a Service/KPI Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- 1.2.4 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

- 2.1 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.
- 2.2 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/KPI Level Performance Measure	Pega Cloud Availability		
Key Indicator	To meet this Service Level, Pega Cloud must be Available for >=99.95% of the Scheduled Service Time		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		
Description	Scheduled Service Time: This Service shall be Available 24 hours per day, 365 days per year (366 days in a leap year).		
Measurement or Service Period	Monthly		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		
	[REDACTED]		
KPI Service Level Thresholds			
Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
>=99.95%	<99.95% and >=99.25% Availability achieved in the Measurement/Service Period	<99.25% and >=98.50% Availability achieved in the Measurement/Service Period	<98.50% Availability achieved in the Measurement/Service Period

Service/KPI Level Performance Measure	Incident Resolution Times Severity 1 – 4
---------------------------------------	------------------------------------------

Key Performance Indicator	<p>To meet this Service Level, the Supplier must achieve the requirements set out in (i) and (ii) below:</p> <p>(i) the percentage or number (as applicable) of Incidents resolved within the target time for that Incident Severity meets or exceeds the target percentage or number (as applicable) specified in the Target Service Level; and</p> <p>(ii) No incident takes longer than the target time.</p>
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

KPI Service Level Thresholds				
Incident Severity Level	Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
Severity 1 Incident	(i) All Incidents have a Resolution Time within the target of four (4) hours (ii) Not applicable	(i) If any one (1) or more Incidents have a Resolution Time over the target of four (4) hours (ii) More than one (1) Incident within the Measurement/Service Period	(i) If any one (1) or more Incidents have a Resolution Time over eight (8) hours (ii) More than two (2) Incidents within the Measurement/Service Period	(i) If more than one (1) Incident has a Resolution Time over twenty (24) hours (ii) More than five (5) Incidents within the Measurement/Service Period
Severity 2 Incident	(i) All Incidents have a Resolution Time within the target of eight (8) hours (ii) Not applicable	(i) If any one (1) or more Incidents have a Resolution Time over the target of four (8) hours (ii) More than one (1) Incident within the Measurement/Service Period	(i) If any one (1) or more Incidents have a Resolution Time over twenty-four (24) hours (ii) More than two (2) Incidents within the Measurement/Service Period	(i) If more than one (1) Incident has a Resolution Time over seventy-two (72) hours (ii) More than five (5) Incidents within the Measurement/Service Period
Severity 3 Incident	(i) >10 incidents in the Measurement/Service Period: 90% or more of the Incidents have a Resolution Time within the target of	(i) >10 incidents within the Measurement/Service Period: more than 10% of Sev 3 Incidents fail the target.	(i) >10 incidents in the Measurement/Service Period: more than 20% of Sev 3 Incidents fail the target.	(i) >10 incidents in the Measurement/Service Period: more than 30% of Sev 3 Incidents fail the target.


	<p>twenty-four (24) hours.</p> <p>(ii) <=10 incidents within the Measurement/Service Period: no more than 1 Sev 3 Incident fails the target.</p>	<p>(ii) <=10 incidents within the Measurement/Service Period: more than one (1) Sev 3 incident fails the target.</p>	<p>(ii) <=10 incidents within the Measurement/Service Period: more than two (2) Sev 3 incidents fail the target.</p>	<p>(ii) <=10 incidents within the Measurement/Service Period: more than three (3) Sev 3 incidents fail the target.</p>
Severity 4 Incident	<p>(i) >10 incidents in the Measurement/Service Period: 90% or more of the Incidents have a Resolution Time within the target of seventy-two (72) hours.</p> <p>(ii) <=10 incidents within the Measurement/Service Period: no more than 1 Sev 4 Incident fails the target.</p>	<p>(i) >10 incidents in the Measurement/Service Period: more than 10% of Sev 4 Incidents fail the target.</p> <p>(ii) <=10 incidents within the Measurement/Service Period: more than one (1) Sev 4 incident fails the target.</p>	<p>(i) >10 incidents in the Measurement/Service Period: more than 20% of Sev 4 Incidents fail the target.</p> <p>(ii) <=10 incidents within the Measurement/Service Period: more than two (2) Sev 4 incidents fail the target.</p>	<p>(i) >10 incidents in the Measurement/Service Period: more than 30% of Sev 4 Incidents fail the target.</p> <p>(ii) <=10 incidents within the Measurement/Service Period: more than three (3) Sev 4 incidents fail the target.</p>

Incident Severity Level	Core Definition	User Impact	Business Criticality
Severity 1 (Sev 1)	The production system is down or inaccessible. Severity 1 only applies to production systems.	> 499 users are impacted	Impact on services preventing Legislatively required outputs, Critical National Infrastructure impacted, or impacting HMRCs disaster response capabilities
Severity 2 (Sev 2)	The reported problem causes disruption of a major feature or function of the system that significantly impacts on production but does not result in extended downtime.	> 499 users are impacted	Impact on go-live of a new HMRC product and/or service.
Severity 3 (Sev 3)	This is the default severity level for submitted Support Requests. The reported problem involves a feature or functional failure that	> 9, < 500 users impacted	N/A

	<p>results in the Pegasystems product not working as described in the documentation. A Severity 3 problem prevents or delays users from performing some tasks.</p>		
<p>Severity 4 (Sev 4)</p>	<p>The reported problem is a presentation or product usability defect with little to no business impact. Severity 4 problems do not prevent users from performing tasks. Examples of Severity 4 problems include typographical errors and user interface element misalignment.</p>	<p>< 10 users impacted</p>	<p>N/A</p>

Service/KPI Level Performance Measure	Problem Assessment Times Severity 1 – 4
Key Performance Indicator	To meet this Service Level, the Supplier must achieve the requirements set out in (i) and (ii) below: (i) the percentage or number (as applicable) of Problems assessed within the target time for that Problem Severity meets or exceeds the target percentage or number (as applicable) specified in the Target Service Level; and (ii) No Problem assessment takes longer than the target time.
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]

	<p>[Redacted content]</p>
--	---------------------------

	
--	------------------------------------------------------------------------------------

KPI Service Level Thresholds – Problem Assessment				
Problem Severity Level	Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
Severity 1 Problem	(i) All Problem records have an Assessment Time within the target of twenty-four (24) hours (ii) Not applicable	<95% and >=90% Problem records achieve target	<90% and >=85% Problem records achieve target	<85% Problem records achieve target
Severity 2 Problem	(i) All Problem records have an Assessment Time within the target of seventy-two (72) hours (ii) Not applicable	<95% and >=90% Problem records achieve target	<90% and >=85% Problem records achieve target	<85% Problem records achieve target
Severity 3 Problem	(i) 95% of Problem records have an Assessment Time within the target of one-hundred-and-twenty (120) hours (ii) Not applicable	<90% and >=85% Problem records achieve target	<85% and >=80% Problem records achieve target	<80% Problem records achieve target
Severity 4 Problem	(i) 95% of Problem records have an Assessment Time within the target of one-hundred-and-twenty (120) hours	<90% and >=85% Problem records achieve target	<85% and >=80% Problem records achieve target	<80% Problem records achieve target

	(ii) Not applicable			
--	---------------------	--	--	--

Problem Severity Level	Core Definition	Delivery Impact	Business Impact	Frequency of occurrence
Severity 1 (Sev 1)	This is a production problem (or critical service development problem) that is leading to multiple high severity production incidents, that would be as severe as a production outage.	Blocking go-live of legislative services, Critical National Infrastructure Services or impacting HMRCs disaster response capabilities	<p>Incidents impact high percentage of HMRC staff using the affected service ($\geq 75\%$)</p> <p>Critical impact on affected business area(s) ability to operate business process</p> <p>Presents a security risk or risk or reputational damage</p>	High likelihood to cause incidents to reoccur
Severity 2 (Sev 2)	Critical issue blocking high priority business functionality, blocking go-live and is a show stopper	Blocking go-live and is a show stopper	<p>Incidents impact high percentage of staff using the affected service ($\geq 50\%$)</p> <p>Disruption to important business function with delays in end to end business process</p> <p>Potential risk of reputational damage or security risk</p>	Likely to cause additional incidents to reoccur
Severity 3 (Sev 3)	Major issue preventing major business use case from being developed.	Major issue preventing major business use case from being developed	Impacts small percentage of staff using the affected service ($< 50\%$)	Unlikely to cause incidents to re-occur
Severity 4 (Sev 4)	Cosmetic issue, nice to have for go-live, documentation issue or other	Cosmetic issue, nice to have for go-live, documentation issue or other	No business impact	No likelihood of reoccurrence

	non-impacting issue.	non-impacting issue		
--	-------------------------	------------------------	--	--

Service/KPI Level Performance Measure	Problem Resolution Times Severity 1 – 4
Key Performance Indicator	To meet this Service Level, the Supplier must achieve the requirements set out in (i) and (ii) below: (i) the percentage or number (as applicable) of Problems resolved within the target time for that Problem Severity meets or exceeds the target percentage or number (as applicable) specified in the Target Service Level; and (ii) No Problem resolution takes longer than the target time.
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]

--	--

KPI Service Level Thresholds – Problem Resolution				
Problem Severity Level	Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
Severity 1 Problem	(i) All Problem records have a Resolution Time within the target of one-hundred-and-twenty (120) hours (ii) Not applicable	Any Severity 1 Problem not resolved within 5 calendar days (120 hours)	Any Severity 1 Problem not resolved within 10 calendar days (240 hours)	N/A
Severity 2 Problem	(i) All Problem records have a Resolution Time within the target of two (2) weeks (14 days) (ii) Not applicable	Any Severity 2 Problem not resolved within 14 calendar days (336 hours)	Any Severity 2 Problem not resolved within 21 calendar days (504 hours)	N/A
Severity 3 Problem	(i) 95% of Problem records have a Resolution Time within three (3) months (90 days)	90% of Problem records achieve resolution time target	85% of Problem records achieve resolution time target	N/A

	(ii) Not applicable			
Severity 4 Problem	(i) 95% of Problem records have a Resolution Time within six (6) months (180 days) (ii) Not applicable	90% of Problem records achieve resolution time target	85% of Problem records achieve resolution time target	N/A

Problem Severity Level	Core Definition	Delivery Impact	Business Impact	Frequency of occurrence
Severity 1 (Sev 1)	This is a production problem (or critical service development problem) that is leading to multiple high severity production incidents, that would be as severe as a production outage.	Blocking go-live of legislative services, Critical National Infrastructure Services or impacting HMRCs disaster response capabilities	Incidents impact high percentage of HMRC staff using the affected service ($\geq 75\%$) Critical impact on affected business area(s) ability to operate business process Presents a security risk or risk or reputational damage	High likelihood to cause incidents to reoccur
Severity 2 (Sev 2)	Critical issue blocking high priority business functionality, blocking go-live and is a show stopper	Blocking go-live and is a show stopper	Incidents impact high percentage of staff using the affected service ($\geq 50\%$) Disruption to important business function with delays in end to end business process Potential risk of reputational damage or security risk	Likely to cause additional incidents to reoccur
Severity 3 (Sev 3)	Major issue preventing major business use	Major issue preventing major business use	Impacts small percentage of staff using the	Unlikely to cause incidents to re-occur

	case from being developed.	case from being developed	affected service (<50%)	
Severity 4 (Sev 4)	Cosmetic issue, nice to have for go-live, documentation issue or other non-impacting issue.	Cosmetic issue, nice to have for go-live, documentation issue or other non-impacting issue	No business impact	No likelihood of reoccurrence

KPI Service Level Thresholds - Accessibility			
Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
The latest evidence (audit report, statement and roadmap) have been received by the Buyer within one month of the most recent Pega version being made available to the Buyer	Evidence received >1 month and <3 months after version release.	Evidence received >3 months after version release.	N/A
No outstanding roadmap fixes that have not been made available to the Buyer within the agreed resolution timelines (defined above in this schedule)	1 or more WCAG 2.2 A fixes outstanding for longer than the agreed resolution timeline and/or 3 or more WCAG 2.2 AA fixes outstanding for longer than the agreed resolution timeline	3 or more WCAG 2.2 A fixes outstanding for longer than the agreed resolution timeline and/or 5 or more WCAG 2.2 AA fixes outstanding for longer than the agreed resolution timeline	N/A

KPI Service Level Thresholds – Security Vulnerabilities			
Target Service Level	Minor KPI Level Failure	Major KPI Level Failure	Critical KPI Level Failure
All listed Compliance Certifications/ Attestations maintained with no lapsed periods	1 or more Compliance Certifications/ Attestations expires, and the Buyer notified within 168 hours	2 or more Compliance Certifications/ Attestations expire and the Buyer not notified after 72 hours	3 or more Compliance Certifications/ Attestations expire and the Buyer not notified after 48 hours
If Certifications/ Attestations expire/lapse, recertification achieved within 1 month	If Certifications/ Attestations expire/lapse, recertification not achieved within 1 month	If Certifications/ Attestations expire/lapse, recertification not achieved within 2 months	If Certifications/ Attestations expire/lapse, recertification not achieved within 3 months

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

- 3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.
- 3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed 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:
 - 3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
 - 3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
 - 3.2.3 details of any Critical Service Level Failures;
 - 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
 - 3.2.5 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
 - 3.2.6 such other details as the Buyer may reasonably require from time to time.
- 3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:
 - 3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;
 - 3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.
- 3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.
- 3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

- 4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Annex 1: Service/KPI Level Performance Measure Specific Definitions

“Agreed Service Time” means the hours specified in the description box in each Service/KPI Level Performance Measure in Annex A to Part A.

“Available” means the Supplier System and/or Service shall be “available” when End Users are able to access and use all its functions at a level that enables them to carry out their normal duties and external customers are able to use its functions.

“End User” means any person authorised by the Buyer to use the IT Environment and/or the Services;

“Scheduled Service Time ” means 24 hours per day, 365 days per year (366 days in a leap year);

"Non-Available" means in relation to the IT Environment or the Services, that the IT Environment or the Services (or a relevant part) are not Available;

“Service Availability” is defined specifically against each individual Service/KPI Level Performance Measure;

“Service Downtime” means any period of time during which any of the Services are not Available;

"Severity Levels" means, for each Service/KPI Level Performance Measure, the bands or levels of performance falling below the Target Service Level which determine the seriousness of the Supplier's failure, as determined in accordance with the tables in Annex A to Part A;

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

1. Definitions

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

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

- 2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.
- 2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.
- 2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

- 3.1 The Supplier's Contract Manager's shall be:
 - 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;
 - 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;
 - 3.1.3 able to cancel any delegation and recommence the position himself; and
 - 3.1.4 replaced only after the Buyer has received notification of the proposed change.
- 3.2 The Buyer may provide revised instructions to the Supplier's Contract 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.
- 3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
 - 5.2.1 the identification and management of risks;**
 - 5.2.2 the identification and management of issues; and
 - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Operational Delivery Board:

Authority Members of Operational Board	[REDACTED]
Supplier Members of Operational Board	[REDACTED]
Start Date for Operational Board meetings	17 th April 2024
Frequency of Operational Board meetings	Monthly
Location of Operational Board meetings	Virtual/MS Teams unless otherwise clarified

Commercial Board:

Authority Members of Commercial Board	[REDACTED]
Supplier Members of Commercial Board	[REDACTED]
Start Date for Commercial Board meetings	Within one month of contract start date
Frequency of Commercial Board meetings	Monthly
Location of Commercial Board meetings	Virtual/MS Teams unless otherwise clarified

Call-Off Schedule 16 (Benchmarking)

1. DEFINITIONS

1.1 In this Schedule, the following expressions shall have the following meanings:

"Benchmark Review"	1 a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;
"Benchmarked Deliverables"	2 any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;
"Comparable Rates"	3 the Charges for Comparable Deliverables;
"Comparable Deliverables"	4 deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark;
"Comparison Group"	5 a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations;
"Equivalent Data"	6 data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;
"Good Value"	7 that the Benchmarked Rates are within the Upper Quartile; and
"Upper Quartile"	8 in respect of Benchmarked Rates, that based on an analysis of Equivalent Data, the Benchmarked Rates, as compared to the range of prices for Comparable

	Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables.
--	----------------------------------------------------------------------------------------------------------------------

2. When you should use this Schedule

- 2.1 The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.
- 2.2 This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.
- 2.3 Amounts payable under this Schedule shall not fall with the definition of a Cost.

3. Benchmarking

3.1 How benchmarking works

- 3.1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.
- 3.1.2 The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.
- 3.1.3 The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.
- 3.1.4 The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.
- 3.1.5 The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.
- 3.1.6 Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.

- 3.1.7 The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

3.2 Benchmarking Process

- 3.2.1 The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:
- (a) a proposed cost and timetable for the Benchmark Review;
 - (b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and
 - (c) a description of how the benchmarker will scope and identify the Comparison Group.
- 3.2.2 The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.
- 3.2.3 The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.
- 3.2.4 Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.
- 3.2.5 Once it has received the Approval of the draft plan, the benchmarker shall:
- (a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:
 - (i) market intelligence;
 - (ii) the benchmarker's own data and experience;
 - (iii) relevant published information; and

- (iv) pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;
 - (b) by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;
 - (c) using the Equivalent Data, calculate the Upper Quartile;
 - (d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.
- 3.2.6 The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.
- 3.2.7 In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:
- (a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);
 - (b) exchange rates;
 - (c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

3.3 **Benchmarking Report**

- 3.3.1 For the purposes of this Schedule "**Benchmarking Report**" shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;
- 3.3.2 The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings. Those findings shall be required to:
- (a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;
 - (b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and
 - (c) include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the

Benchmarked Deliverables are, individually or as a whole,
Good Value.

- 3.3.3 The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance with Clause 24 (Changing the contract).

Call-Off Schedule 18 (Background Checks)

1. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

2. Definitions

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

3.1.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

3.1.2 Notwithstanding Paragraph 2.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):



- (a) carry out a check with the records held by the Department for Education (DfE);
- (b) conduct thorough questioning regarding any Relevant Convictions; and
- (c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

Relevant persons conducting activities within the governance of this contract must hold and maintain the required security clearance level for the role undertaken.

	
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]




[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]





[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
------------	------------

	  
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	[REDACTED]
[REDACTED]	[REDACTED]

Call-Off Schedule 23 (Supplier-Furnished Terms)

Part 1A Non-COTS Third Party Software

Terms for licensing of non-COTS third party software are detailed in Annex 1.

Part 1B COTS Software

Terms for licensing of COTS software are detailed in Annex 2

Part 1C Software as a Service (SaaS) Terms

Terms for provision of a Software as a Service solution are detailed in Annex 3.

Part 1D Software Support and/or Maintenance Terms

Terms for provision of Software Support and/or Maintenance services are detailed in Annex 4.

Part 1E Pegasystems Services Terms

Terms for provision of a Pegasystems Services are detailed in Annex 5.

Annex 1

Not Relevant

Annex 2

Not Relevant

Annex 3 Software as a Service (SaaS) Terms

[Redacted]

[Redacted]

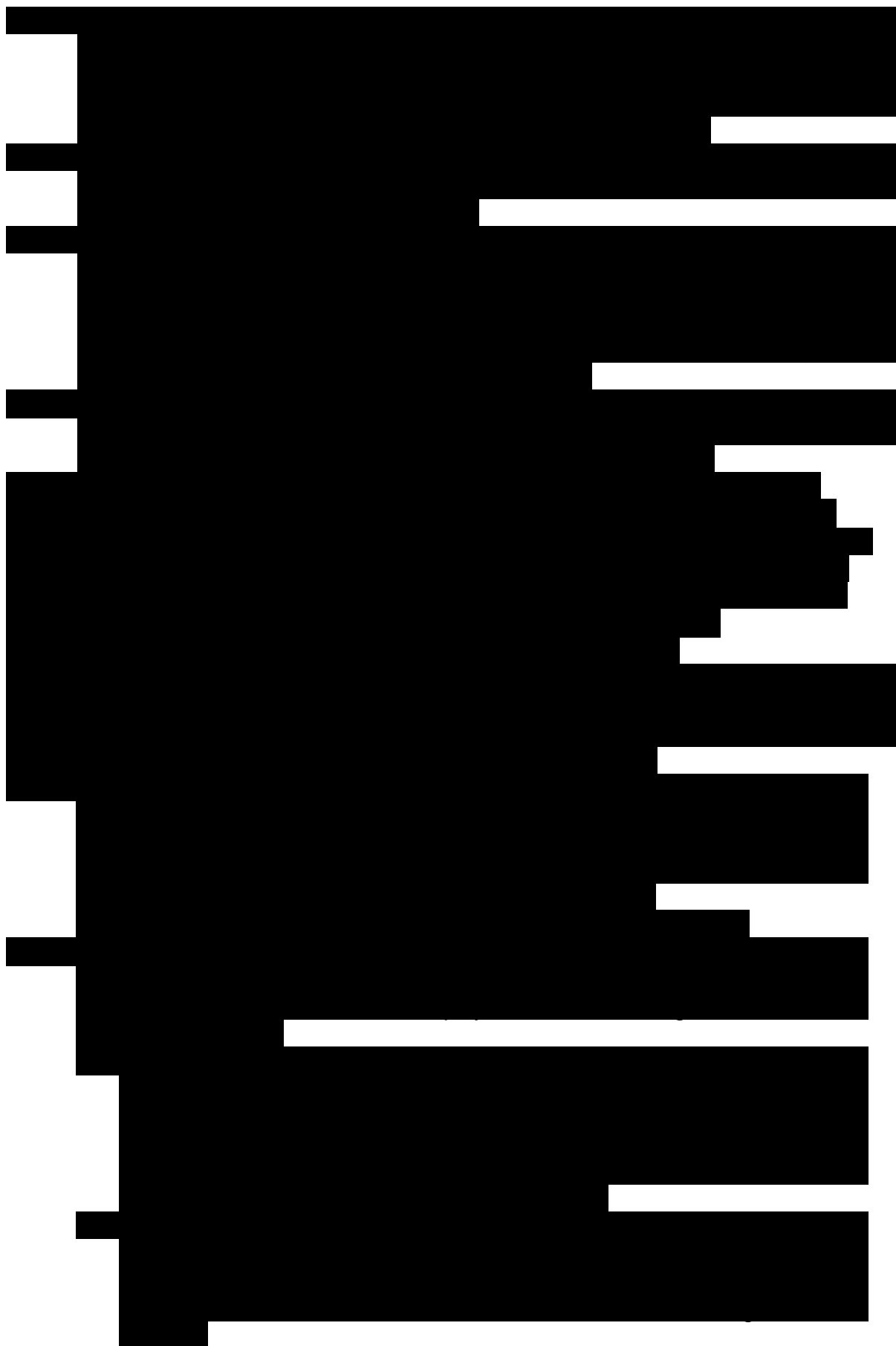
[Redacted]

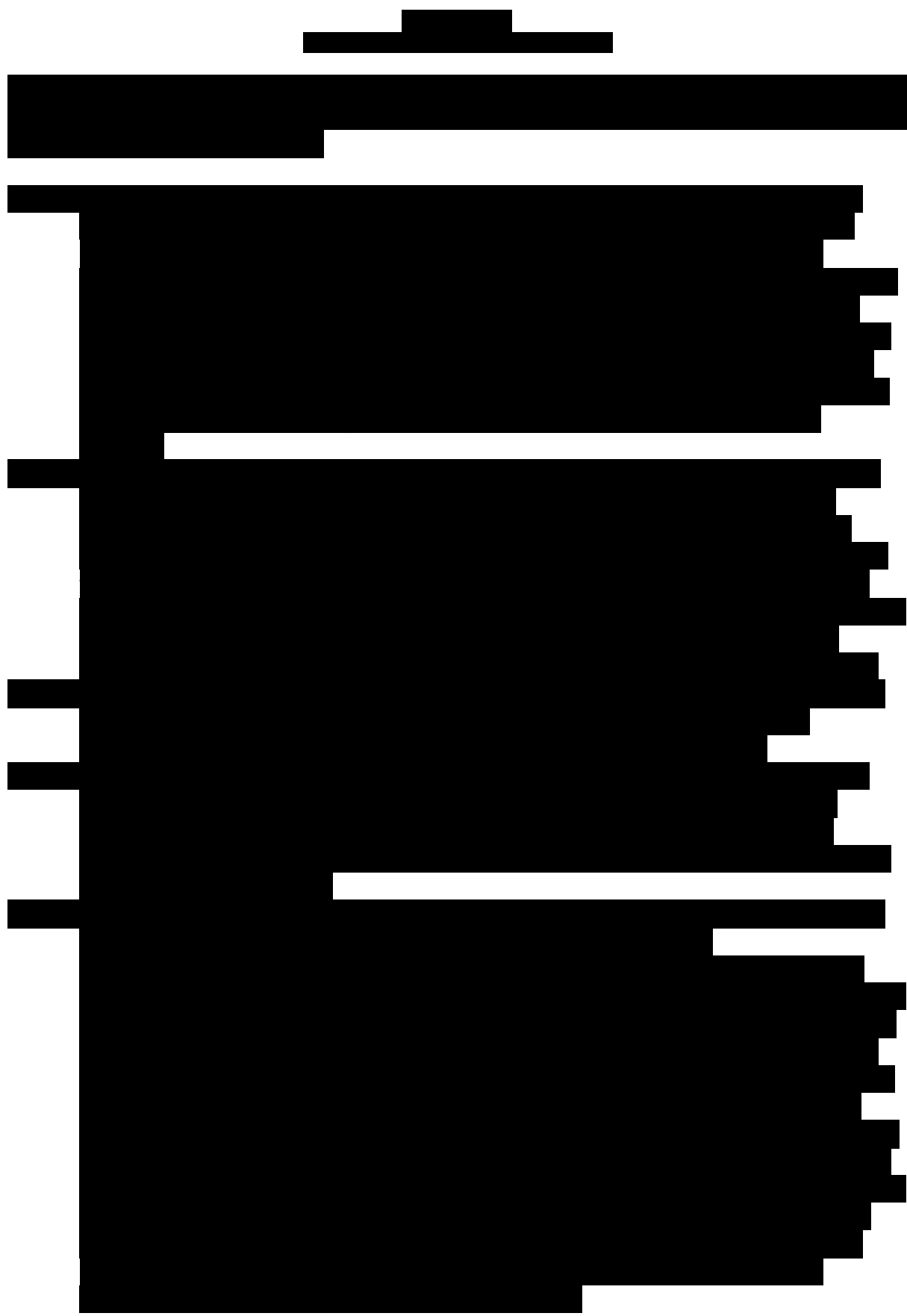
[REDACTED]



[REDACTED]

The table contains multiple rows of data, but the content is almost entirely obscured by black redaction boxes. Only a few horizontal white bars are visible, indicating the structure of the data.







[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Additional Schedule (HMRC Terms)

1. Definitions

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

“Connected Company” in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;

“Control” the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;

“Prohibited Transaction” a) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description otherwise payable by the Supplier or a Connected Company on or in connection with the Charges; or

b) which would be payable by any Key Subcontractor and its Connected Companies on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract,

other than transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business;

“Purchase Order Number” the Buyer's unique number relating to the supply of the Deliverables;

“Supporting Documentation” sufficient information in writing to enable the Buyer to reasonably verify the accuracy of any invoice; and

**“Tax
Compliance
Failure”**

where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC’s “Test for Tax Non-Compliance”, as set out in Annex 1 (as amended and updated from time to time), where:

- (a) the “Economic Operator” means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Paragraph 5.3; and
- (b) any “Essential Subcontractor” means any Key Subcontractor.

2. Exclusion of certain Core Terms and terms of Schedules

2.1. When the Parties have entered into a Call-Off Contract which incorporates the terms of this Call-Off Schedule 23, the following Core Terms are modified in respect of that Call-Off Contract (but are not modified in respect of the Framework Contract):

2.1.1. Clauses 31.1, 31.2, 31.3 and 31.4(d) of the Core Terms do not apply to that Call-Off Contract, but for the avoidance of doubt, the remainder of Clause 31.4 of the Core Terms shall continue to apply to the Call-Off Contract; and

2.1.2. Clause 7.2 of the Core Terms does not apply to that Call-Off Contract.

2.2. When the Parties have entered into a Call-Off Contract which incorporates the terms of this Call-Off Schedule 23, the following Joint Schedules are modified in respect of that Call-Off Contract (but are not disapplied in respect of the Framework Contract):

2.2.1. The definition of “Occasion of Tax Non-Compliance” contained in Joint Schedule 1 (Definitions) does not apply to that Call-Off Contract; and

2.2.2. paragraph 5(d) of Joint Schedule 11 (Processing Data) does not apply to that Call-Off Contract.

3. Charges, Payment and Recovery of Sums Due

3.1. The Supplier shall invoice the Buyer as specified in Clause 4 of the Core Terms as modified by any Framework Special Terms or any Call-Off Special Terms.

3.2. In addition to the provisions of Clause 4 of the Core Terms and any applicable Framework Special Term or Call-Off Special Term, the Supplier shall procure a Purchase Order Number from the Buyer before any Deliverables are supplied. Should the Supplier supply Deliverables without a Purchase Order Number:

3.2.1. the Supplier does so at its own risk; and

3.2.2. the Buyer shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

3.3. The Supplier shall submit each invoice and any Supporting Documentation required in accordance with Clause 4 of the Core Terms and any applicable Framework Special Term or Call-Off Special Term, as directed by the Buyer from time to time, either:

3.3.1. via the Buyer's electronic transaction system as an Electronic Invoice;

4. Warranties

4.1. The Supplier represents and warrants that:

4.1.1. in the three years prior to the Effective Date, it has complied with all applicable Law related to Tax in the United Kingdom and in the jurisdiction in which it is established;

4.1.2. it has notified the Buyer in writing of any Tax Compliance Failure it is involved in; and

4.1.3. no proceedings or other steps have been taken (nor, to the best of the Supplier's knowledge, are threatened) for:

4.1.3.1. the winding up of the Supplier;

4.1.3.2. the Supplier's dissolution; or

4.1.3.3. the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue,

and the Supplier has notified the Buyer of any profit warnings it has issued in the three years prior to the Effective Date.

4.2. If the Supplier becomes aware that any of the representations or warranties under Paragraphs 4.1.1, 4.1.2 and/or 4.1.3 have been breached, are untrue or misleading, it shall immediately notify the Buyer in sufficient detail to enable the Buyer to make an accurate assessment of the situation.

4.3. In the event that the warranty given by the Supplier in Paragraph 4.1.2 is materially untrue, this shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and 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.

5. Promoting Tax Compliance

5.1. The Supplier shall comply with all Law relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

5.2. The Supplier shall provide to the Buyer the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to that person supplying any material Deliverables under the Contract.

5.3. Upon a request by the Buyer, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor of the Supplier engaged in supplying Deliverables under the Contract.

5.4. If, at any point during the Call-Off Contract Period, there is a Tax Compliance Failure, the Supplier shall:

5.4.1. notify the Buyer in writing within five (5) Working Days of its occurrence; and

5.4.2. promptly provide to the Buyer:

5.4.2.1. details of the steps which the Supplier is taking to resolve the Tax Compliance Failure and to prevent it from recurring, together with any mitigating factors that it considers relevant; and

5.4.2.2. such other information in relation to the Tax Compliance Failure as the Buyer may reasonably require.

5.5. The Supplier shall indemnify the Buyer against any liability for Tax (including any interest, penalties or costs incurred) of the Buyer in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Contract.

5.6. Any amounts due under Paragraph 5.5 shall be paid not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Buyer. Any amounts due under Paragraph 5.5 shall not be subject to clause 11.2 of the Core Terms.

5.7. Upon the Buyer's request, the Supplier shall promptly provide information which demonstrates how the Supplier complies with its Tax obligations.

5.8. If the Supplier:

5.8.1. fails to comply with Paragraphs 5.1, 5.4.1 and/or 5.7 this may be a material breach of the Contract;

5.8.2. fails to comply with a reasonable request by the Buyer that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Paragraph 5.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in a Tax Compliance Failure this shall be a material breach of the Contract; and/or

5.8.3. fails to provide acceptable details of steps being taken and mitigating factors pursuant to Paragraph 5.4.2 this shall be a material breach of the Contract;

and any such material breach shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and 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.

5.9. In addition to those circumstances listed in clause 15.2 to 15.4 of the Core Terms, the Buyer may internally share any information, including Confidential Information, which it receives under Paragraphs 5.2 to 5.4 (inclusive) and 5.7.

6. Use of Off-shore Tax Structures

6.1. The Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place any Prohibited Transactions, unless the Buyer otherwise agrees to that Prohibited Transaction.

6.2. The Supplier shall notify the Buyer in writing (with reasonable supporting detail) of any proposal for the Supplier, its Connected Companies, or a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall include reasonable supporting detail and make the notification within a

reasonable time before the Prohibited Transaction is due to be put in place.

6.3. If a Prohibited Transaction is entered into in breach of Paragraph 6.1, or circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Buyer. The Parties shall agree (at no cost to the Buyer) any necessary changes to any such arrangements by the undertakings concerned (and the Supplier shall ensure that the Key Subcontractor shall agree, where applicable). The matter will be resolved using clause 34 of the Core Terms if necessary.

6.4. Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Paragraphs 6.2 and 6.3 shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and 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.

7. Data Protection and off-shoring

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

7.1.1. not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

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

7.1.1.2. the Data Subject has enforceable rights and effective legal remedies;

7.1.1.3. 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

7.1.1.4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

7.2. Failure by the Processor to comply with the obligations set out in Paragraph 7.1 shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and 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.

8. Commissioners for Revenue and Customs Act 2005 and related Legislation

- 8.1. The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 (“CRCA”) to maintain the confidentiality of Government Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to a prosecution under Section 19 of CRCA.
- 8.2. The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in the Official Secrets Acts 1911 to 1989 and the obligations set out in Section 182 of the Finance Act 1989. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to prosecution under those Acts.
- 8.3. The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Deliverables. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of the Supplier’s obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.
- 8.4. The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Staff who will have access to, or are provided with, Government Data in writing of the obligations upon Supplier Staff set out in Paragraphs 8.1, 8.2 and 8.3. The Supplier shall monitor the compliance by Supplier Staff with such obligations.
- 8.5. The Supplier shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Buyer upon demand.
- 8.6. In the event that the Supplier or the Supplier Staff fail to comply with this Paragraph 8, the Buyer reserves the right to terminate the Contract as if that failure to comply were an event to which clause 10.4.1 of the Core Terms applies.

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: ("X")
 - 1) The Economic Operator or Essential Subcontractor (EOS)
 - 2) Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*¹;
 - 3) Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:
 - . Fraudulent evasion²;
 - a. Conduct caught by the General Anti-Abuse Rule³;
 - b. Conduct caught by the Halifax Abuse principle⁴;
 - c. Entered into arrangements caught by a DOTAS or VADR scheme⁵;

¹ <https://www.iasplus.com/en/standards/ifrs/ifrs10>

² 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

³ "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

⁴ "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

⁵ A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as

- d. Conduct caught by a recognised 'anti-avoidance rule'⁶ being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;
- e. Entered into an avoidance scheme identified by HMRC's published Spotlights list⁷;
- f. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

- . In respect of (a), either X:

1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure⁸; or,
2. Has been charged with an offence of fraudulent evasion.

- i. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

⁶ The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

⁷ Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: <https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight>

⁸ The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

- ii. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
- iii. In respect of (f) this condition is satisfied without any further steps being taken.
- iv. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

Annex 2 Form

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: [for Supplier to insert Contract reference number and contract date] ((‘the Agreement’))

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Government Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Government Data provided to me.

SIGNED:
FULL NAME:
POSITION:
COMPANY:
DATE OF SIGNATURE:

[REDACTED]



Statement of Work

Pegasystems Limited

[Project Title]

[Quarter, Financial Year]

[Description of Work]

Date:	
Version:	
HMRC Ref:	
Pegasystems Ref:	

Contents

1. Summary	207
2. Description of the Services Required	208
3. Responsibilities	209
4. Deliverables	209
5. Knowledge Transfer & Enablement	210
6. Payment Schedule	210
7. Change Control	211
8. Performance Standards and Quality Assurance	Error! Bookmark not defined.
9. Locations of work and travel	211
10. Off boarding and Termination	211
11. Overtime and on-call	211
12. Reporting and Communications	211
13. Approvals	212
14. Appendices	213
Appendix 1 – Change Control Form	213

Summary

Project/Programme Title	Insert Project Title
Agreement	Insert BoS agreement details here
SOW Duration Dates	Start date: DD/MM/YY End date: DD/MM/YY
Total Coverage of SOW	Time and Materials

This Statement of Work (“SOW”) document is made by and between:

1. Pegasystems Limited (“Pegasystems”) – **Supplier**

AND

2. HM Revenue and Customs (“HMRC”) – **Customer**

This SOW is subject to the terms and conditions of the Agreement for the Provision of Consulting Services agreement between HMRC and Pegasystems Limited [INSERT BOS Call off details here]

Any terms used in this SOW but not defined shall have meaning ascribed to such a term in the Agreement. In the event of a conflict between the terms of the Agreement and this SOW, this SOW shall prevail.

Description of the Services Required

Pegasystems will provide skilled resources to support the Delivery of activities aligned to sprints within the SOW period.

These sprints have been aligned to the standard Customer Engagement Pega Delivery team projects and 'live service' operations sprint cadence.

The below sprint dates are shown for reference:

[Insert sprint dates if relevant]

These resources will engage in various tasks as described below as directed by the Customer.

Responsibilities

The activities described below are provided as an indication of the likely activities to be completed in these sprints, however these activities will be refined, prioritised, and agreed with HMRC.

Any tasks not expressly mentioned in the Description of Services Required above and Responsibilities below shall therefore be regarded as being out of scope of this SOW.

Pegasystems will:

- Bullet-pointed list of activities and obligations Pegasystems are responsible for

HMRC will:

- Bullet-pointed list of activities and obligations HMRC are responsible for

Deliverables

Pegasystems shall be responsible for its obligations under this SOW, ensuring the successful delivery of the following sprints.

[Insert sprint dates if relevant]

Content of each sprint will be agreed with the Business Product Owner and Head of Product and Innovation as part of the standard sprint cadence meetings.

Change Control

Any change that impacts either the scope of services, timeline or fees shall require both parties to mutually execute a Change Control (see Appendix 1) prior to the delivery of services continuing.

Locations of Work and Travel

Due to current remote working practices in line with the HMRC's policy, the resources shall be based both remotely and on-site at office location(s), based on mutual agreement. HMRC will provide all the required accounts, hardware and software to allow the Pegasystems supplier resources to connect to all required environments during the remote working period.

Off boarding and Termination

Upon signing this SOW either party may terminate this SOW for convenience by providing 30 days' advanced written notice.

In the event of termination, Pegasystems shall invoice HMRC for all work performed up to the effective date of termination plus incurred and pre-paid reasonable expenses where applicable.

Overtime and On-Call

No overtime or on-call will be applicable, unless agreed in writing between HMRC and Pegasystems. During periods of product deployments, there may be a requirement for activities outside of HMRC's Standard Operating Hours (07:00 – 20:00) to minimise IT disruption to users.

HMRC may request Pegasystems to provide resources to support these successful deployments to meet customer demand, or on instruction from Government. Acceptance of any such request is subject to mutual agreement in writing.

Reporting and Communications

HMRC and Pegasystems will meet monthly to discuss delivery and progress against the SOW, any performance or behavioural issues and any alterations or changes required to any documentation.

Approvals

This SOW and the Agreement constitute the entire understanding of the parties with respect to the Services to be performed under this SOW.

Customer (HM Revenue and Customs)		Supplier (Pegasystems Limited)	
Signature		Signature	
Name		Name	
Title		Title	
Date		Date	

Appendices`

Appendix 1 – Change Control Form

This Change Control (CR-XXXXX) references CR-XXXXX effective from

DD/MM/YYYY between Pegasystems Limited and HMRC. Change Control effective date:
DD/MM/YYYY.

Description of Changes

Reason for Change: For example changes to Scope, additional roles and rates etc.

In the event that both parties agree for additional services to be delivered then the following table shall apply:

Role	Estimated Hours	Rate per Hour	Estimated Fees
Total Estimated Hours		Total Estimated Fees	
		Estimated Expenses	
		Total Estimated Fees and Expenses	

Expenses shall be chargeable as incurred and will be invoiced on a monthly basis / No Expenses shall be chargeable as they are included in the labour rate.

No services shall be delivered against this Change Control until it has been fully executed.

Authorisation

All other terms and conditions of the original SOW (CR-XXXXX) remain unchanged. This Statement of Work and the Agreement constitute the entire understanding of the parties with respect to the Services to be performed under this Statement of Work.

Customer (HM Revenue and Customs)		Supplier (Pegasystems Limited)	
Signature		Signature	
Name		Name	
Title		Title	
Date		Date	