



# Crown Commercial Service

## G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Part A: Order Form .....	2
Schedule 1: Services .....	12
Schedule 2: Call-Off Contract charges .....	12
Part B: Terms and conditions .....	13
Schedule 3: Collaboration agreement .....	32
Schedule 4: Alternative clauses .....	44
Schedule 5: Guarantee .....	49
Schedule 6: Glossary and interpretations .....	57
Schedule 7: GDPR Information .....	68

### Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

<b>Digital Marketplace service ID number</b>	631381468003501
<b>Call-Off Contract reference</b>	25090

<b>Call-Off Contract title</b>	CCMP Expert Services Partner Transition
<b>Call-Off Contract description</b>	Provision of Expert Services Partner Transition services, including the provision of cloud contact centre implementation, transition, configuration and enhanced support services.
<b>Start date</b>	30 September 2022
<b>Expiry date</b>	29 February 2024
<b>Call-Off Contract value</b>	£3,262,339 plus VAT with extensions of a value up to £880,000 plus VAT.
<b>Charging method</b>	Fixed price
<b>Purchase order number</b>	

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

<b>From the Buyer</b>	Department for Work and Pensions DWP Commercial Directorate Finance Group 5th Floor 2 St Peter's Square Manchester M2 3AA
<b>To the Supplier</b>	Anana Limited 12th floor Blue Fin Building 110 Southwark Street London SE1 0SU Company number: 04309449
<b>Together the 'Parties'</b>	

### Principal contact details

#### For the Buyer:

[Redacted]

#### For the Supplier:

[Redacted]

### Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on <b>30 September 2022</b> and is valid for <b>18 months</b> .
-------------------	---

<b>Ending (termination)</b>	<p>The notice period for the Supplier needed for Ending the CallOff Contract is at least <b>90</b> Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of <b>30</b> days from the date of written notice for Ending without cause (as per clause 18.1).</p>
<b>Extension period</b>	<p>This Call-off Contract can be extended by the Buyer for <b>one</b> period of up to 12 months, by giving the Supplier <b>3 months</b> written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.</p>

### Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

<b>G-Cloud lot</b>	<p>This Call-Off Contract is for the provision of Services under:</p> <ul style="list-style-type: none"> <li>• Lot 1: Cloud hosting</li> <li>• Lot 2: Cloud software</li> <li>• Lot 3: Cloud support</li> </ul>
<b>G-Cloud services required</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: <input type="checkbox"/> <b>Setup and migration</b></p> <ul style="list-style-type: none"> <li>• <b>Quality assurance and performance testing</b></li> <li>• <b>Training</b></li> <li>• <b>Ongoing support</b></li> </ul> <p>The precise Services to be delivered by the Supplier shall be identified in individual Statements of Work as agreed in Variations to Schedule 1 of this Call-Off contract.</p>

<b>Additional Services</b>	<p>It is contemplated that the following additional services may be required from the Supplier:</p> <ul style="list-style-type: none"> <li>□ Variations to CAN101 (Implementation Services) to account for changes in CCMP delivery timelines or to</li> </ul>
	<p>instruct the Supplier to deliver additional Services that are necessary for the delivery of the DC3 platform;</p> <ul style="list-style-type: none"> <li>• Steady-state run support of the DC3 platform for a period of up to 12 months if required as a contingency measure;</li> <li>• Extension of the Services for a period of up to 12 months to enable the exit and transition of the Services to DWP or an alternative supplier.</li> </ul>
<b>Location</b>	<p>The Services will be delivered either remotely or at DWP offices at 2 St Peter's Square, Manchester, M3 2AA</p>
<b>Quality standards</b>	<p>The quality standards required for this Call-Off Contract are <b>specified in Schedule 1 Services.</b></p>
<b>Technical standards:</b>	<p>The technical standards used as a requirement for this CallOff Contract are <b>specified in Schedule 1 Services.</b></p>
<b>Service level agreement:</b>	<p>The service level and availability criteria required for this CallOff Contract are <b>stated in Schedule 1 Services.</b></p>
<b>Onboarding</b>	<p>Onboarding requirements as set out in Schedule 1 Services.</p>
<b>Offboarding</b>	<p>Offboarding requirements as set out in Schedule 1 Services.</p>

<b>Collaboration agreement</b>	Not applicable
<b>Limit on Parties' liability</b>	<p>The annual total liability of either Party for all Property Defaults will not exceed <b>£3,000,000</b>.</p> <p>The annual total liability for Buyer Data Defaults will not exceed <b>£3,000,000</b> or <b>150%</b> of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other Defaults will not exceed the greater of <b>£1,500,000</b> or <b>125%</b> of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
<b>Insurance</b>	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>• professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)</li> <li>• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.</li> </ul>
<b>Force majeure</b>	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than <b>60</b> consecutive days.</p>

<b>Audit</b>	<p>The Buyer shall have the right to audit the Supplier on an annual basis to ensure the accuracy of the Charges.</p>
<b>Buyer's responsibilities</b>	<ol style="list-style-type: none"> <li>1) DWP will provide high-level design documentation to the Supplier.</li> <li>2) Relevant resource attendance at scheduled workshops.</li> <li>3) Information required for the Supplier to produce documentation.</li> <li>4) All relevant project documentation e.g. HLSO, Comms plan RAAIDD, RACI</li> </ol>
	<ol style="list-style-type: none"> <li>5) Relevant licences for access to third party systems.</li> <li>6) Provision of laptops where required to access DWP systems.</li> </ol>
<b>Buyer's equipment</b>	<p>The Buyer's equipment to be used with this Call-Off Contract includes <b>laptop devices</b>.</p> <p>Reason <b>to ensure secure access to DWP systems as required</b>.</p>

## Supplier's information

<p><b>Subcontractors or partners</b></p>	<p>The following is a list of the Supplier's Subcontractors or Partners.</p> <ul style="list-style-type: none"> <li>• Genesys Europe B.V.</li> <li>• Verint Systems UK Ltd</li> <li>• Sabio Ltd</li> </ul> <p>Each of Subcontractor or Partner will perform professional services in support of the delivery of the Services in Schedule 1.</p>
--	---

## Call-Off Contract charges and payment


The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

<p><b>Payment method</b></p>	<p>[Redacted]</p>
<p><b>Payment profile</b></p>	<p>The payment profile for this Call-Off Contract is <b>monthly</b> in arrears.</p>

<p><b>Invoice details</b></p>	<p>The Supplier will post paper invoices monthly in arrears to the Buyer SSCL address and send a PDF version of the invoice to the SSCL email address below in accordance with the appropriate agreed Payment Profile.</p> <p>The Supplier must be prepared to use electronic purchase to pay (P2P) routes, including catalogue and e-invoicing. The Supplier must be prepared to work with the Buyer to set up and test all electronic P2P routes. This may involve creating technical ordering and invoice files, including working with our ERP system service suppliers and systems.</p> <p>The Buyer will pay the Supplier within 30 days of receipt of the valid PDF invoice at SSCL.</p>
-------------------------------	---



<p><b>Who and where to send invoices to</b></p>	<p>Hard copies and electronic invoices shall be sent and emailed respectively to:</p> <p>[Redacted]</p>
<p><b>Invoice information required</b></p>	<p>All invoices must include purchase order number, contract reference and Buyer's reference details.</p> <p>The invoice format will follow the standard Supplier invoice format mirroring the necessary information as described in Part B, clause 7.5 of the Call Off Contract.</p> <p>The Buyer will pay the Supplier within thirty (30) calendar days of receipt of a valid invoice, submitted in accordance with this paragraph, the payment profile set out in Schedule 2 and the provisions of this Call-Off Contract.</p>
<p><b>Invoice frequency</b></p>	<p>Unless otherwise stated in Schedule 2 or via a Variation, invoices will be sent to the Buyer monthly in arrears.</p>
<p><b>Call-Off Contract value</b></p>	<p>The total value of this Call-Off Contract is £3,262,339 plus VAT with extensions of a value up to £880,000 plus VAT.</p>

<p><b>Call-Off Contract charges</b></p>	<p>The breakdown of the Charges is set out below.</p> <p>[Redacted]</p> <p>The detailed mapping of deliverables to milestones is located in Schedule 1 Services.</p> <p>Upon completion of all deliverables associated with a milestone, the Supplier shall submit a milestone acceptance certificate (in the attached form) to the Buyer. Milestone acceptance certificates will be required in respect of each milestone for formal certification prior to invoicing.</p> <div style="text-align: center;">  <p>Milestone Certificate.docx</p> </div> <p>Day rate pricing is located in Schedule 2 – Call-Off Contract Charges.</p>
---	--

**Additional Buyer terms**

<p><b>Performance of the Service and Deliverables</b></p>	<p>All milestones and associated deliverables are stated in Schedule 1 – Services.</p>
<p><b>Guarantee</b></p>	<p>Not required</p>

<b>Warranties, representations</b>	In addition to the incorporated Framework Agreement clause 4.1, the Supplier shall provide such warranties and representations as set out in Schedule 1 Services.
--	---

**Supplemental requirements in addition to the Call-Off terms**

- The Supplier shall not include restrictive covenant(s) in its contract(s) with its Subcontractor(s) that would prevent or impede any such Subcontractor(s) from contracting directly or indirectly with the Buyer in the event the Buyer Ends the Call Off Contract and/or any individual Statement of Work (in whole or in part) for any reason. This clause shall survive termination of the Call Off Contract.

**“Good Security Practice”** shall

mean:

- a. The technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology);
- b. Security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and
- c. The Government’s security policies, frameworks, standards and guidelines relating to Information Security.

**“Information Security Questionnaire”** shall mean the Buyer’s set of questions used to audit and on an ongoing basis assure the Supplier’s compliance with the Buyer’s Security Requirements.

**“Security Test”** shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.

**1. Principles of Security**



The Supplier shall at all times comply with the Buyer's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

## **2. Security Accreditation**

The Supplier shall be accredited to ISO27001 standard.

## **3. Cyber Essentials**

The Supplier shall obtain and maintain certification to Cyber Essentials (the "Cyber Essentials Certificate") in relation to the Services during the Term of this Call-Off Contract.

## **4. Risk Management**

4.1 The Supplier shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Term of the Call-Off Contract which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Buyer's Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk

Management Policy to the Buyer upon request within 10 Working Days of such request. The Buyer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Buyer's Security Requirements. The Supplier shall, at its own expense, undertake those actions required in order to implement the changes required by the Buyer within one calendar month of such request or on a date as agreed by the Parties.

4.2 The Supplier shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the

Supplier's Systems Environment or in the threat landscape or (iii) at the request of the Buyer. The Supplier shall provide the report of the Risk Assessment to the Buyer, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Buyer within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

	<p>4.3 If the Buyer decides, at its absolute discretion, that any Risk Assessment does not meet the Buyer's Security Requirements, the Supplier shall repeat the Risk Assessment</p>
--	--





within one calendar month of such request or as agreed by the Parties.

4.4 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer's own risk management processes regarding the Services.

4.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 3. Any failure by the Supplier to comply with any requirement of this paragraph 3 (regardless of whether such failure is capable of remedy), shall constitute a Material Breach entitling the Buyer to exercise its rights under clause 18.5.

### **5. Information Security Questionnaire**

The Supplier shall complete the information security questionnaire in the format stipulated by the Buyer (the "**Information Security Questionnaire**") at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one calendar month from the date of request.

### **6. Security Tests**

6.1 The Buyer, or an agent appointed by it, may undertake

Security Tests in respect of the Supplier's Systems Environment after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Supplier's Security Requirements, the Supplier shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Buyer at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Buyer as the Buyer may reasonably require.

6.2 The Supplier shall conduct Security Tests to assess the

Information Security of the Supplier's Systems Environment and, if requested, the Buyer's Systems Environment. In relation to such Security Tests, the Supplier shall appoint a third party which in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Supplier's Systems Environment or in the Buyer's System

	Environment or (iii) at the request of the Buyer which request
--	--

may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Buyer. The Supplier shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Buyer in its absolute discretion.

6.3 The Buyer shall be entitled to send the Buyer's Representative to witness the conduct of any Security Test. The Supplier shall provide to the Buyer notice of any Security Test at least one month prior to the relevant Security Test.

## **7. Security Governance Review Meetings**

The Buyer may schedule regular security governance review meetings which the Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

## **8. Security Policies and Standards**

8.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with the Buyer Security Policies and Standards set out below.

8.2 Notwithstanding the foregoing, the Buyer's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Variation to this Call-Off Contract, any change in the Buyer's Security Requirements resulting from such Variation (if any) shall be agreed by the Parties in accordance with the Variation process.

8.3 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

**9. Buyer Security Policies and Standards**

The Security Policies are published on:

<https://www.gov.uk/government/publications/dwpprocurement-security-policies-and-standards> unless specified otherwise:

- a) Acceptable Use Policy
- b) Information Security Policy
- c) Physical Security Policy
- d) Information Management Policy
- e) Email Policy
- f) Technical Vulnerability Management Policy
- g) Remote Working Policy
- h) Social Media Policy
- i) Forensic Readiness Policy
- j) SMS Text Policy
- k) Privileged Users Security Policy
- l) User Access Control Policy
- m) Security Classification Policy
- n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018

(published on

<https://www.gov.uk/government/publications/hmg-personnelsecurity-controls>)

p) NCSC Secure Sanitisation of Storage Media

(published on

<https://www.ncsc.gov.uk/guidance/securesanitisation-storage-media>)

## **10. Cyber Security Information Sharing Partnership**


10.1 The Supplier may become a member of the Cyber Security Information Sharing Partnership in accordance with the recommendations by the NCSC during the Term of this Call-Off Contract. The Supplier may participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

10.2 Where the Supplier becomes a member of the Cyber

Security Information Sharing Partnership, it shall review the NCSC weekly threat reports on a fortnightly basis and implement appropriate recommendations in line with the Supplier's Risk Management Policy.

## **11. Security Clearance**

Security clearance requirements are identified in Schedule 1.

	<p style="text-align: center;"><b>12. Offshoring</b></p> <p>The Supplier has confirmed that the Services do not fall within the definition of Offshoring as stated in the Buyer’s Offshoring Policy.</p> <p>The Supplier shall at all times comply with the Buyer’s Offshoring Policy. In the event that Offshoring is envisaged at any point during the Term of this Call-Off Contract, the Supplier shall immediately notify the Buyer and the Parties shall discuss and the Buyer shall agree the appropriate requirements for the Supplier to satisfy its obligations under this clause and the Buyer’s Offshoring Policy (which will require an Enterprise Security Risk Management assessment being undertaken by the Buyer) prior to any Offshoring taking place.</p> <div style="text-align: center;">  <p>DWP OFFSHORING POLICY V4.0 A GUIDE FOR DWP CONTRACTORS</p> <p style="font-size: small;">14 March 2016</p> </div>
<p><b>Alternative clauses</b></p>	<p>Not applicable</p>

<p><b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b></p>	<p><input type="checkbox"/> The parties agree that clauses 4.2 and 4.5 shall be amended as follows:</p> <p>4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer. The Supplier must confirm in writing prior to the commencement of each Statement of Work that all resources deployed to deliver the</p>
---	---



services are employees (with PAYE tax and NI deducted at source).

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35 or is unable to confirm that the Services are delivered by resources with PAYE tax and NI deducted at source.

- The parties agree that clauses 11.2 and 11.3 shall be amended as follows:

11.2 Any Project Specific IPRs created under this Call-Off Contract is owned by the Buyer. The Buyer grants the Supplier a non-exclusive, revocable, royalty free licence to use the Project Specific IPRs and any Buyer Background IPRs where necessary for the purposes of the Supplier fulfilling its obligations under the Call-off Contract during the Term. The Supplier shall have the right to sub license the Sub-contractor's use of the Project Specific IPRs and any Buyer Background IPRs embedded within the Project Specific IPRs solely for the same purpose as the Supplier. At the end of the Term the Supplier shall cease use of the Project Specific IPRs and any Buyer Background IPRs.

11.2.1 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use any Supplier Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the Project Specific IPRs as open source.

- The Parties agree that the following clauses shall be added as 11.9 and 11.10 to the Call off Terms:

11.9 The Buyer shall promptly notify the Supplier of any claim or demand which is made, brought or threatened against the Buyer in respect of the infringement or alleged infringement of any Intellectual Property Right by reason of the Use\* or possession of the Services and/or Deliverables by the Buyer. The Supplier shall at its own expense conduct all negotiations and any litigation arising in connection with any claim for breach of Intellectual Property Rights in materials supplied or licensed by the Supplier, provided always that the Supplier:-

	<p>a) shall consult the Buyer on all substantive issues which arise during the conduct of such litigation and negotiations;</p> <p>b) shall take due and proper account of the interests of the Buyer; and</p> <p>c) shall not settle or compromise any claim without the Buyer's prior written consent (not to be unreasonably withheld or delayed).</p> <p>11.10 The Buyer shall, at the cost and request of the Supplier provide to the Supplier all reasonable assistance for the purpose of contesting any claim or demand made or action brought against the Buyer or the Supplier for infringement or alleged infringement of any Intellectual Property Right in connection with the performance of the Supplier's obligations under the Call-off Contract. * "Use" means use for the Buyer's own internal business purposes and only to the extent necessary to receive the benefit of the Services and/or Deliverables.</p> <p>The parties agree that the definition of "<b>Background IPRs</b>" in Schedule 6 shall be amended as follows:</p> <p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>• owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified as part of the Services or otherwise) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>• created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
<b>Public Services Network (PSN)</b>	Not applicable
<b>Personal Data and Data Subjects</b>	See Schedule 7 Annex 1

## 1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a CallOff Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

## 2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

<b>Signed</b>	Supplier	Buyer
<b>Name</b>	[Redacted]	[Redacted]
<b>Title</b>	[Redacted]	[Redacted]
<b>Signature</b>	[Redacted]	[Redacted]
<b>Date</b>	September 26, 2022   13:55 BST	September 26, 2022   07:16 PDT

# Schedule 1: Services

## 1. INTRODUCTION

### 1.1. Background

DWP currently have a managed service contract with BT PLC, that delivers the largest contact centre operation in Europe. The 32,000+ trained advisors perform multiple services based in our 170+ contact centres, for the citizens of the United Kingdom. The initial term of the BT contract was due to expire in March 2022 and DWP executed the optional +1 year extension option. There is a contractual provision for a further +1 year extension as a contingent option (subject to Cabinet Office and Treasury approvals).

DWP has established the Contact Centre Modernisation Programme (CCMP) to deliver a new DWP managed Digital Channels Contact Centre (DC3). DWP are looking for an expert services partner to deliver the remaining platform implementation activities. This will include services to support the transition of all managed services out of BT to an in-house function. The services will also include support post transition to complete knowledge sharing with and support during the early life of the migrations.

## 2. OVERVIEW OF DWP REQUIREMENTS

### Implementation Needs

#### Third Party Vendors

DWP require an expert services partner that has the capability to work with all Genesys and Verint products.

#### Requirement Refinement

DWP has a need to deliver a transformation that will leave little to no requirement for agent workforce retraining, and cause the least amount of disruption to service. DWP wish to maintain a like for like or better approach. Understanding that the new version of the Genesys Multicloud CX Private Edition may not be directly comparable with current systems every effort should be made to maintain these goals and deliver within timescales. As part of initial discovery work a number of features and functionality 'deltas' from the old system to the new platform have been identified. The specific requirements and deltas will need refinement and are deemed essential aspects of core Business Groups successfully serving the Citizens making contact with them. We therefore require all capabilities to be delivered ready for the first business group to complete migration. Any issues with integration will need to be identified and resolved.

#### Historical Data

There are legal requirements for maintaining historic call and transcription data within DWP and also requirements to follow the DWP data retention policy. This forms the basis for the requirement to migrate data from BT into the new platform, making it accessible to operational users.

#### Call Recording

Integration between Genesys and Verint call recording is required. There is a requirement for the Supplier to work with Genesys and Verint to ensure that appropriate integration between the applications is achieved.

#### Service Lines and Business Configuration

Ownership of all the Business Configuration Build elements is still to be determined in full, section 4.9 covers the high level view. We do have a requirement to complete the creation of / to build all service lines (350 approx.). At present DWP require all the lines built by the Supplier with the option to have the business configuration layer also added by them. This shall cover the following items but not exclusive to; Baseline service line config set up, with options that can be added to them; BG Config - Specific info, building the skills, opening hours, voice messaging, adding agents etc.

## **Design Documentation & Knowledge Transfer**

[Redacted]

**3. WAYS OF WORKING** DWP have two active build squads and one self service automation paused to be completed after transition. These squads are working in two-week sprints and are following the agile methodology. In addition to these we also have a Dev Ops squad that wraps around to act as the enabler for all squads. The Supplier will own and run 3 squads (detail found in section 3.2.1) working collaboratively with the DWP squads.

### **3.1. Principles**

The Supplier shall attend the following meetings/ceremonies. It is expected that a designated individual will attend the meetings below, and that relevant information will be cascaded to the rest of the Supplier team. We will also require at the completion of milestones where are able to see completed works via a show & or tell meeting.

[Redacted]

### **3.2. Squads**

The work is currently organised into squads based on technology areas, with a separate squad for testing. The Supplier will continue to work in squads determined by the technology as set out in 3.2.1 and the DWP Build area in 3.2.2 defined as 'Squad'

#### **3.2.1. Supplier Squads**

- Core and SSO
- Routing
- Recording

#### **3.2.2. DWP Squads**

- Self-service – paused until migration completed
- Workforce Management
- Operational Data
- Dev Ops

#### **3.2.3. Testing**

- Test Manager embedded within the DWP test squad
- Testers embedded in Supplier & DWP squads

### **3.3. Environments to be Delivered**

There will be four types of environments in scope for the Supplier to hand over to DWP as part of the Programme, with the ability for multiple Development and Test environments to be deployed on demand via automation:

- Development
- Test
- Staging (Supplier responsible for meeting the Site Reliability Engineer (SRE) Stage Gate 1 Acceptance Criteria) SRE were introduced to provide protection for Live Services, ensuring services are built with the right characteristics as they progress through the software development life cycle (SDLC) into Production.
- Production (Supplier responsible for meeting the SRE Stage Gate 2 Acceptance Criteria).  
NOTE: Privileged access in some areas will mean the Supplier will be required to provide services delivered by SC Cleared personnel.

A fifth 'Sandpit' environment (not including Verint applications) has been created on DWP's infrastructure by the Supplier with the purpose of this environment to share knowledge on Genesys Multicloud CX Private Edition and build learnings with DWP teams. The Supplier will periodically deliver updates to DWP for the Sandpit when new services are ready.

Each environment / the build must:

- Adhere to the SRE guidelines and DWP best practises
- Include integrations to support full functionality
- Adhere to Digital Workplace Application Deployment Standards
- Adhere to DWP Security Standards
- Be fully documented and handed over to DWP using confluence.

### **3.4. Progress Updates and Reporting**

The Supplier shall deliver the following progress updates:

a) Weekly progress report by squad detailing the following information:

- Progress
- Challenges
- Successes
- Opportunities □            Actions

b) Weekly Exec report covering a combined view of the overall delivery detailing the following information:

- Progress
- Challenges
- Successes
- Opportunities □            Actions

c) Monthly performance review report submitted prior to the monthly performance review detailing the following information:

- Actions from previous meeting
- Progress update on each milestone
- Plan acceleration activities
- Knowledge transfer plan

- Issues requiring escalation or leadership support (from either party)
- Commercial summary
- Change requests / variations  Any other business

d) On an annual basis the Supplier shall provide details of all open source software used in the delivery of its services.

### 3.5. RACI

The Supplier shall adhere to the roles and responsibilities stated in the attached RACI.



CCMP RACI

## 4. SERVICES

### 4.1. Supplier Roles

The Supplier is required to provide the following

ROLE	RESPONSIBILITY
Programme Manager	<ul style="list-style-type: none"> <li>• Will be the responsible for planning and monitoring the overall programme from a Supplier perspective,</li> <li>• Ensuring that programme controls are managed throughout the lifecycle of the programme.</li> <li>• Risks &amp; Issues management</li> <li>• Own and drive mitigating actions where possible</li> <li>• Resource management across all Supplier squads</li> <li>• Stakeholder management providing regular updates and communications.</li> <li>• First point of contact for any internal or DWP escalations regarding the programme.</li> <li>• Providing a weekly report / completion overview</li> </ul>
Project Manager	<ul style="list-style-type: none"> <li>• The primary point of contact for DWP,</li> <li>• Responsible for helping to ensure that all the prerequisites and deliverables tasks assigned to the Supplier are undertaken within the designated timescales,</li> <li>• Daily management of all the appropriate Supplier resources, together with communicating project progress in the agreed formats.</li> </ul>
ROLE	RESPONSIBILITY
	<ul style="list-style-type: none"> <li><input type="checkbox"/> Will attend the daily build stand up calls to request help when required</li> </ul>
Technical Leads	<ul style="list-style-type: none"> <li>• Technical owners of the design, build, technical configuration across all squads</li> <li>• Production of the associated design documentation set.</li> </ul>



Genesys Consultant	<ul style="list-style-type: none"> <li>□ Responsible for working with DWP to define and document operational design and configuration of Genesys features</li> </ul>
Verint Consultant	<ul style="list-style-type: none"> <li>□ Responsible for working with to define and document operational design and configuration of Verint features</li> </ul>
Verint Engineer	<ul style="list-style-type: none"> <li>□ Responsible for deployment of the various components within the Verint System, together with subsequent DWP functional and system testing.</li> </ul>
Dev Ops Consultant	<ul style="list-style-type: none"> <li>□ Responsible for working on the technical configuration associated to; automated CI/CD pipelines and supporting processes for deploying the solution and any associated technical configuration.</li> </ul>
Lead Test Consultant	<ul style="list-style-type: none"> <li>• Responsible for leading the day-to-day activities of the test team members, including the managing of an ongoing project(s).</li> <li>• Responsible for defining processes for testing each phase of the testing lifecycle.</li> </ul>
Test Consultant	<ul style="list-style-type: none"> <li>• Responsible for reviewing software requirements and</li> <li>• Preparing test scenarios for each test phase/test concern. □ Responsible for executing test scenarios □ Analysis of test results.</li> </ul>

#### 4.2. Work Streams

The Supplier will be responsible for the following work streams. The below tables in section 4 show the component services for this work stream, the RACI item it forms part of, and the technical dependencies:

##### 4.2.1. Voice Inbound (Non-Agent)

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Genesys Authentication	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	<ul style="list-style-type: none"> <li>• Ansible Playbook updated to contain specified areas and is confirmed as being available.</li> <li>• All Design documentation updated to contain specified areas and is confirmed as being available.</li> </ul>
Voice Microservices	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	
Tenant Service	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	
Web Services and Applications	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> </ul>	
DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
	<ul style="list-style-type: none"> <li>□ Genesys dependency integration</li> </ul>	All documentation and code produced has been reviewed

Designer	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys routing</li> <li>• Genesys dependency integration</li> </ul>	and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.
Genesys Voice Platform	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	

#### 4.2.2. Voice Inbound (Agent)

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Workspace Web Edition	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys routing</li> <li>• Workspace web edition</li> <li>• Outgoing call features</li> <li>• Hierarchy, users and permissions</li> <li>• Genesys dependency integration</li> </ul>	<ul style="list-style-type: none"> <li>• Ansible Playbook updated to contain specified areas and is confirmed as being available.</li> <li>• Design documentation updated to contain specified areas and is confirmed as being available.</li> </ul> <p>All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.</p>
WebRTC Media Service	<ul style="list-style-type: none"> <li>• Genesys applications</li> <li>• Genesys routing</li> <li>• Outgoing call features</li> </ul>	
Simple Workflow to Agent	<input type="checkbox"/> Genesys routing	
Provision Voice Routing Config	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys routing</li> </ul>	
Provision Final Voice Workflow	<input type="checkbox"/> Genesys routing	
Telemetry	<ul style="list-style-type: none"> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	

#### 4.2.3. Chat (Agent)

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Universal Contact Service	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	<input type="checkbox"/> Ansible Playbook updated to contain specified areas and is confirmed as being available.
DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA

Digital Channels	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	<input type="checkbox"/> Design documentation updated to contain specified areas and is confirmed as being available.  All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.
Provision Chat Routing Config	<ul style="list-style-type: none"> <li>• Genesys applications</li> <li>• Genesys routing</li> <li>• Outgoing call features</li> </ul>	
Provision Final Chat Workflow	<input type="checkbox"/> Genesys routing	
Interaction Server	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	

#### 4.2.4. Reporting

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Genesys Info Mart	<input type="checkbox"/> Genesys databases <input type="checkbox"/> Genesys applications <input type="checkbox"/> Genesys dependency integration	<ul style="list-style-type: none"> <li>• Ansible Playbook updated to contain specified areas and is confirmed as being available.</li> <li>• Design documentation updated to contain specified areas and is confirmed as being available.</li> <li>• All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.</li> </ul>
Genesys Pulse	<input type="checkbox"/> Genesys databases <input type="checkbox"/> Genesys applications <input type="checkbox"/> Genesys dependency integration	
Genesys Customer Experience Insights	<input type="checkbox"/> Genesys databases <input type="checkbox"/> Genesys applications <input type="checkbox"/> Genesys dependency integration	
Billing Data Service	<input type="checkbox"/> Genesys databases <input type="checkbox"/> Genesys applications	

#### 4.2.5. Dialler

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
CX Contact	<ul style="list-style-type: none"> <li>• Genesys databases</li> <li>• Genesys applications</li> <li>• Genesys dependency integration</li> </ul>	<input type="checkbox"/> Ansible Playbook updated to contain specified areas and is confirmed as being available.

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
		<ul style="list-style-type: none"> <li>Design documentation updated to contain specified areas and is confirmed as being available.</li> <li>All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.</li> </ul>

#### 4.2.6. Call Recording

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Call Recording	<ul style="list-style-type: none"> <li>Verint databases</li> <li>Verint applications</li> <li>Verint call recording integration</li> <li>Verint call recording features</li> <li>Verint LEAP (ad hoc data retention extension)</li> </ul>	Verint Technical Design documentation updated to contain specified areas and is confirmed as being available.
Key Management Server	<input type="checkbox"/> Verint encryption of call recordings	Verint Technical Design documentation updated to contain specified areas and is confirmed as being available.
Import Manager	<input type="checkbox"/> Verint historical data migration	Verint Technical Design documentation updated to contain specified areas and is confirmed as being available.

#### 4.2.7. Interaction Analytics

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Quality Monitoring	<ul style="list-style-type: none"> <li>Verint databases</li> <li>Verint applications</li> <li>Verint quality management</li> </ul>	<input type="checkbox"/> Verint Functional Design documentation updated to contain specified areas and is confirmed as being available.
Performance Management	<ul style="list-style-type: none"> <li>Verint databases</li> <li>Verint applications</li> <li>Verint performance management</li> </ul>	
Speech Analytics	<ul style="list-style-type: none"> <li>Verint databases</li> <li>Verint applications</li> <li>Verint speech analytics</li> </ul>	

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Verint Desktop Application	☐ Desktop software	☐ Verint Desktop Deployment Plan updated to contain specified areas and is confirmed as being available.

#### 4.2.8. SSO

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Genesys Authentication	☐ SSO	<ul style="list-style-type: none"> <li>• Ansible Playbook updated to contain specified areas and is confirmed as being available.</li> <li>• Design documentation updated to contain specified areas and is confirmed as being available.</li> <li>• All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.</li> </ul>
Web Services and Applications	☐ SSO	
Workspace Web Edition	☐ SSO	
Verint Applications	☐ SSO	Verint Technical Design documentation updated to contain specified areas and is confirmed as being available.

#### 4.2.9. Operational Observability

DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Genesys Authentication	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	<ul style="list-style-type: none"> <li>• Ansible Playbook updated to contain specified areas and is confirmed as being available.</li> <li>• Design documentation updated to contain specified areas and is confirmed as being available.</li> </ul>
Voice Microservices	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	

Tenant Services	<ul style="list-style-type: none"> <li>□ Genesys application and container logging configuration</li> </ul>	confirmed as being available.
DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
	<ul style="list-style-type: none"> <li>□ Genesys dependency integration</li> </ul>	<ul style="list-style-type: none"> <li>□ All documentation and code produced has been reviewed and confirmed as meeting DWP standards and approved by the CCMP Build Approval Board.</li> </ul>
Web Services and Applications	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Designer	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Genesys Voice Platform	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Workspace Web Edition	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
WebRTC Media Service	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Telemetry	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Universal Contact Service	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Digital Channels	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
Interaction Server	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	

Genesys Info Mart	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
DELIVERABLES	RACI ITEMS	ACCEPTANCE CRITERIA
Genesys Customer Experience Insights	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	
CX Contact	<ul style="list-style-type: none"> <li>• Genesys application and container logging configuration</li> <li>• Genesys dependency integration</li> </ul>	

#### 4.3. Other RACI items

The following items are listed in the RACI and will also require some collaborative work with third party suppliers to deliver the services. This may be in the form of meetings or workshops to ensure protection of delivery dates:

- Genesys Backend Integration
- Genesys Desktop Integration
- Nectar
- Zephyr
- TestComplete
- Hardware SIP phones & headsets

#### 4.4. Training

The Supplier shall provide sufficient training to DWP super users to ensure their readiness to support their Business Group to effectively operate the systems for their business area. The grid below is an example of the minimum number of areas which will need to be covered with the Super users (experienced DWP staff) from the Business Groups. It is not known at this point how many Super users will be needed, but the volume will not be less than 28 as this is equal to 1 per Business Group.

DESCRIPTION
<p style="text-align: center;"><b>Speech Analytics Delta</b></p> <ul style="list-style-type: none"> <li>• Review of changes in Speech Analytics between 15.1 and 15.2</li> <li>• Walks through the process for creating and applying a Phonetic Boost</li> </ul>
<p style="text-align: center;"><b>Interactions Administration</b></p> <ul style="list-style-type: none"> <li>• Administration of the Interactions application</li> <li>• Options for transcription rule administration</li> <li>• Options for recording deletion</li> </ul>
<p style="text-align: center;"><b>Interactions End User Delta</b></p> <ul style="list-style-type: none"> <li>• Reviews changes to the Interactions/Quality component</li> <li>• Looks at updates to export functionality within the application</li> </ul>

### Ad Hoc Reports

- Examines the process of creating ad hoc reports
- Reviews the process for scheduling ad hoc reports

### Verint technical knowledge transfer

#### 4.5. Requirements by Milestones

The below tables from section 4.5.1 - 4.5.9 consist of technical tasks broken down from the individual workstreams detailed in section 4.2.1 – 4.2.9. The user stories can be found embedded in section 4.6 (Functional Requirements) which provides the specifics of what is being delivered from these activities excluding customisations yet to be determined.

##### 4.5.1. Voice Inbound (Non-Agent)

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
Development	Core - Platform	Pipeline provisioning of Environment
Development	Core - Platform	Pipeline provisioning of Contact Centre
Development	Core - Platform	Pipeline provisioning of Datacentre(s)
Development	Core - Platform	Agent Setup Application UI is Available
Development	Core - Platform	GWS Provisioning APIs are Available
Development	Core - Platform	Designer Application UI is Available
Development	Core - Platform	Designer APIs are available
Development	Core - Config	Pipeline provisioning of queue pointing to "Simple voice Workflow"
Development	Core - Config	Pipeline provisioning of trunk on Multi-cloud platform to SBC
Development	Routing	Pipeline provisioning of "Simple Voice Workflow"
Development	Routing	Pipeline provisioning of a queueing announcement
Development	Routing	Routing will consist of a single announcement on a continuous loop
Test	Core - Platform	Completed load test (1000 concurrent calls) against the "Simple Voice Workflow"

##### 4.5.2. Voice Inbound (Agent)

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
Development	Core - Platform	SCCB to Client JIRA WWE mapping sheet
Development	Core - Platform	WWE UI is available
Development	Core - Config	Pipeline provisioning of queue pointing to "Simple voice Workflow to Agent"



Development	Core - Config	Pipeline provisioning of multiple Agents and supporting config
Development	Core - Config	Pipeline provisioning of Supervisor and supporting config
Development	Core - Config	Pipeline provisioning of a hold announcement
Development	Core - Config	Pipeline provisioning of NotReady Reason Codes
Development	Routing	Pipeline provisioning of "Simple Voice Workflow to Agent"
Development	Routing	Routing will consist of a single announcement on a continuous loop until the call is delivered to an agent
<b>ENVIRONMENT</b>	<b>SQUAD</b>	<b>ACCEPTANCE CRITERIA</b>
Development	Core - Config	Pipeline provisioning of queues pointing to "Final Voice Workflow"
Development	Core - Config	Pipeline provisioning of Folder Structure
Development	Core - Config	Pipeline provisioning of Permissions
Development	Core - Config	Pipeline provisioning of Roles
Development	Core - Config	Pipeline provisioning of Access Groups
Development	Routing	Pipeline provisioning of all required business config (e.g. disposition codes, skills, opening times, etc) on 5 test queues
Development	Routing	SCCB to Client JIRA Routing mapping sheet
Development	Routing	Completed designed call flows in Confluence
Test	Routing	Completed load test (1000 concurrent calls) against the "Final Voice Workflow"

#### 4.5.3. Chat (Agent)

<b>ENVIRONMENT</b>	<b>SQUAD</b>	<b>ACCEPTANCE CRITERIA</b>
Development	Core - Platform	Widget UI available to be loaded on to a test web site
Development	Core - Config	Pipeline provisioning of queue pointing to "Final Chat Workflow"
Development	Core - Config	Pipeline provisioning of chat endpoint
Development	Routing	Pipeline provisioning of "Final Chat Workflow"
Development	Routing	Pipeline provisioning of all required business config (e.g. disposition codes, skills, opening times, etc) on queues
Development	Routing	SCCB to Client JIRA Routing mapping sheet
Development	Routing	Completed designed chat interaction flows in Confluence

#### 4.5.4. Reporting (Pulse and CXI)

<b>ENVIRONMENT</b>	<b>SQUAD</b>	<b>ACCEPTANCE CRITERIA</b>
Development	Core - Platform	Pipeline deployment of Pulse

Development	Core - Platform	Pipeline deployment of CXI
Development	Core - Platform	Pulse UI is Available
Development	Core - Platform	Pipeline deployment of Validation Pulse wallboard and dashboard
Development	Core - Platform	Validation Pulse wallboard and dashboard show the correct information
Development	Core - Platform	CXI UI Is Available
Development	Core - Platform	OOTB Voice CXI Report shows the correct information

#### 4.5.5. Dialler

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
Development	Core - Platform	CX Contact UI Is Available
Development	Core - Platform	Create and Upload a Calling List
Development	Core - Platform	Create and Start a Campaign

#### 4.5.6. Call Recording

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
<b>N/A</b>	<b>Recording</b>	<b>Technical Design signed off</b>
Development	Recording	Development environment build completed
Development	Recording	Development environment testing completed
Test	Recording	Test environment build completed
Test	Recording	Test environment testing completed
Staging	Recording	Staging environment build completed
Staging	Recording	Staging environment testing completed
Production	Recording	Production environment build completed
Production	Recording	Production environment testing completed

#### 4.5.7. Interaction Analytics

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
<b>N/A</b>	<b>Recording</b>	<b>Functional Design signed off</b>
Development	Recording	Development environment Functional Testing completed
Test	Recording	Test environment Functional Testing completed
Staging	Recording	Staging environment Functional Testing completed
Production	Recording	Production environment Functional Testing completed

**4.5.8. SSO**

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
Development	Core - Platform	As a single user I can SSO to access; Agent Setup, Designer, WWE

**4.5.9. Operational Observability**

ENVIRONMENT	SQUAD	ACCEPTANCE CRITERIA
Development	Core - Platform	Pod logging is being delivered to the centralised logging solution
Development	Core - Platform	Pod and service metrics are being delivered to centralised Prometheus

**4.6. Functional Requirements**

The Supplier is required to ensure that the contact centre platform build complies with the specified functional requirements in the attached “Functional Requirements” file.



Functional

requirements V1.1907

**4.7. Project Management Services**

The Supplier will assign a specific Programme Manager and supporting Project Managers to help ensure the successful delivery of the Solution. The Supplier project managers will be resourced to this project 100% of their time.

DWP expect that the Project Management engagement is based on the ways of working details provided in section 3.1 which will be a mixture of onsite and remote attendance at key points throughout the project life cycle.

There will be a requirement to be available for project reviews at least once a week, with further reviews when required.

Standard practice of being available to answer calls and email during working hours is expected of all project leaders such as Programme Manager and Project Managers. All documentation should meet DWP quality ISO9001 standards and align with all accessibility WCAG (Web content accessibility guidelines 2.1) requirements.

The Project Manager will be responsible for the following items as indicated in the table below:

PROJECT DELIVERABLES	NOTES
Template Documents	Template formats agreed at project commencement
Project Plan	MS Project

Risks, Actions, Assumptions, Issues, Decisions, Dependencies (RAAIDD) Log	
Change Controls/Log	
Contact Matrix	
Project Notes	
Sign-offs	
Project Reviews	One per Week
Out of Hours Activities	For activities designated as requiring to be completed outside standard business hours.

#### 4.8. Testing

The scope of the CCMP Testing requirement is the successful delivery of CCMP Programme Test Function, as detailed in this Scope of Works. The following sections define the testing to be undertaken by the Supplier and the testing to be undertaken by DWP. The Supplier shall use DWP's Zephyr Enterprise systems to store all testing information.

##### 4.8.1. Test Delivery Needs

The Supplier will work closely with the Programme's Delivery Teams to:

- a) Provide quality assurance of the code being developed. Define and create test cases and detailed scripts within the CCMP test tooling applications to assure User Story requirements.
- b) Manage Testing services across all CCMP Build Squads (planning, generating test scripts, execution and defect management).
- c) Validate the scope of the Epics and User Stories documented in Jira in both the existing backlog and within each subsequent build sprint.
- d) Produce and document test plans aligned to each sprint.
- e) Document test plan within Zephyr
- f) Produce and document test scripts which accurately align with User Stories across the test tooling.
- g) Undertake testing of User Stories across all Build teams
- h) Perform test execution across all Supplier managed squads, and responsible for defect resolution and re-testing

##### 4.8.2. Defect and Incident Management

All defects or incidents identified through testing need to be managed and logged in Jira. The Supplier will work collaboratively with the Build teams and DWP partners to resolve issues in line with the specified priority level.

##### 4.8.3. DWP Test Requirements

- a) Plan, define, execute and report on test cases, and the subsequent defect management of test cases within;
  - i. Test Environments
  - ii. Staging Environment
  - iii. Production Environment
  - iv. Support and facilitate DWP ORT & UAT phases

- b) Testing to be aligned to the CCMP Test Strategy, CI/CD planning and release cycle
- c) Alignment with Build teams ways of working methods and assets across business analysis, Epics & User Stories, test management and defect analysis
- d) Ensure test cases documented and completed as a minimum 2 sprints refined ahead of the associated build activity within Zephyr Test Management application.
- e) Produce and maintain the test plans and reports in line with the Build team sprint cycles.
- f) Document Test cases within Zephyr, Nectar CX / Nectar AX and Test complete
- g) Engage with the build teams and programme stakeholders, product owners and technical team resources throughout the delivery of the solution build.
- h) Management and leadership of the Test team across both the Suppliers and DWP Build squads, working closely with the Product Manager, Test Engineers and Project Managers whilst reporting into the CCMP Lead Test Manager
- i) Lead and manage the testing of the defect/issue and resolution process, across all sprints.
- j) Delivery of progress reports, providing Programme trackers and ad-hoc reports as necessary
- k) Ensure JIRA Epics and User Stories are correctly aligned to Zephyr, Test Complete and Nectar CX test scripts as appropriate

#### 4.9. Business Configuration

The Supplier shall deliver the following business configuration and extraction services:

- a) Technical consultancy and support for a hybrid responsibility data migration model based on an Export, Transform, Load process from existing NGCC Genesys and Verint environments, into DC3 Genesys and Verint environments (WFM migration is excluded from scope)
- b) EXTRACT: DWP will assume responsibility for the 'Extract' phase but we will required the supplier to tell us prescriptively which data, in which format, needs exporting to achieve a successful like for like migration into the DC3 platform
- c) TRANSFORM & VERIFY: The Supplier will need to consult with DWP on Transform activities including validation of content to pre-empt loading and testing/operational failures
- d) LOAD: The Supplier will be required to perform the data load using their own tooling capability which must first be assured by DWP Lead Architect and Security Architect. Partner will need to ensure sufficient config across each of our 3 environments (Multiple Dev, Test, Staging Environments) in order to successfully transform and pass testing for all required configuration and business data into the Production environment
- e) LOAD: The Supplier will be required to perform all required testing, and root cause analysis relating to load failures, provide feedback into the transform phase, and take responsibility to load and re-test, based on any corrective activity, through to successful testing/proof of load
- f) SUPPORTING ACTIVITY: The Supplier will be required to perform handover into our delivery and run teams, and provide consultancy for any early life support issues. This includes documentation, knowledge transfer etc.
- g) We are not prescriptive on which tools are to be used to load the data providing the correct assurance process has been followed through the afore mentioned DWP Architects
- h) Supplier will be required to conform to DWP Transition policies and ways of working

#### 4.10. Transition

- a) The Supplier shall provide transition support services to the Buyer in line with the Business Group transition plan stated in 4.10.1.
- b) The Supplier shall work closely with the Buyer to ensure close Supervision of the Business Group users at go-live.
- c) The Supplier will be expected to provide a feedback mechanism back into the Build Teams for refinement of the delivery.
- d) The Supplier will perform dual running with the incoming ESP Run supplier to conduct Knowledge transfer & upskilling to ESP Run in the required format/location throughout the duration of the contract
- e) Refinement of the expected support processes (& Knowledge Management).
- f) The Supplier will provide Enhanced early monitoring and assist in scrutiny and refinement of any in-life Event Management thresholds
- g) Review of onboarding success with each Business Group and service capability owners

##### 4.10.1. Business Group Transition Plan



#### 4.11. Early Life Support

The Supplier shall deliver Early-Life Support services in accordance with the following requirements:

- a) Provision of Early Life Support of the platform from the transition of the first Business Group(s) until 3 months after transition of the final Business Group(s).
- b) Enhanced Reporting and Proactive analysis throughout.
- c) Transparency with regards to how we work together and with whom.
- d) Resolution of all incidents assigned to the Supplier within the service levels specified in 4.11.2.

#### 4.11.1. Incident Categorisation

All Incidents are prioritised, dependant on the level of impact on the Buyer. There are 4 priority levels and the appropriate priority will be selected as details are gathered about the incident.

##### Priority 1 (P1)

- Complete failure of a business-critical application and/or business critical service affecting all users at one or more key sites, or all users at two or more secondary sites, or all users within a specific business group at one or more sites; or
- Delay to, or the inaccurate production of business-critical outputs.

##### Priority 2 (P2)

- Complete failure of a business-critical application and or business critical service affecting all users at a single secondary site; or
- Partial failure of a business-critical application and or business critical Service affecting all users at one or more key sites, or all users at two or more secondary sites, or all users within a specific business group at one or more sites; or
- Complete failure of a secondary application and/or secondary service affecting all users at one or more key sites.
- The Buyer reserves the right to raise the priority of a ticket where an Incident meets these Priority 2 criteria but is deemed to have a wider impact and/or urgency.

##### Priority 3 (P3)

- Partial failure of a business-critical application and or business critical service affecting all users at a single secondary site; or
- Complete failure of a secondary application and or secondary service affecting all users at one or more secondary sites; or
- Partial failure of a secondary application and or secondary service affecting all users at one or more key sites; or
- Partial failure of a secondary application and or secondary service affecting all users at two or more secondary sites; or
- Failure of a piece of equipment.
- The Buyer reserves the right to raise the priority of a ticket where an Incident meets these Priority 3 criteria but is deemed to have a wider impact and/or urgency.

##### Priority 4 (P4)

- Partial failure of a secondary application and or secondary service affecting all users at one secondary site; or
- Incident or occurrence which is not a Priority 1, Priority 2, or Priority 3

#### 4.11.2. Incident Response Service Levels

The Supplier shall resolve all incidents assigned to them within the associated service levels:

Priority	Service Level
<b>P1</b>	2 hours - 24/7/365
<b>P2</b>	8 hours - 24/7/365
<b>P3</b>	20 Working Hours - 0800-1800 Mon-Fri (excluding Public Holidays*)
<b>P4</b>	31 Working Hours - 0800-1800 Mon-Fri (excluding Public Holidays*)

#### 4.11.3. Knowledge Transfer

The Supplier shall deliver knowledge transfer activities as defined below to facilitate knowledge transfer to DWP and any replacement supplier(s):

- a) transfer all training material and provide appropriate training to those DWP and/or replacement supplier(s) staff responsible for internal training in connection with the provision of the Services;
- b) enable DWP and/or any replacement supplier(s) to shadow the relevant Supplier personnel delivering the Services;
- c) transfer to DWP and/or any replacement supplier(s) all knowledge reasonably required for the provision of the Services which may, as appropriate, include information, records and documents;
- d) provide DWP and/or any replacement supplier(s) with access to such members of the Supplier's personnel as have been involved in the design, development, provision or management of the Services and who are still employed or engaged by the Supplier or its sub-contractors;
- e) to facilitate the transfer of knowledge from the Supplier to DWP and/or any replacement supplier(s), the Supplier shall provide a detailed explanation of the procedures and operations used to provide the Services, the Change Management process and other standards and procedures to the operations personnel of the Buyer and/or any replacement supplier(s);
- f) the information which the Supplier shall provide to DWP and/or any replacement supplier(s) shall include:
  - i. copies of up-to-date procedures and operations manuals;
  - ii. all product information;
  - iii. all agreements with third party suppliers of goods and services which are to be transferred to DWP and/or any replacement supplier(s);
  - iv. information regarding any unresolved faults and/or incidents in progress as well as those expected to be in progress at the end of the term and the Parties have agreed to transfer the faults/incidents to DWP and/or any replacement supplier(s);
  - v. system design and configuration;
  - vi. system backups and restores;
  - vii. data backups and restores;
  - viii. functions performed at specific times (e.g. period end);
  - ix. Incident Management - a review of DWP's incidents over the term of the Services;
  - x. Problem Management - a review of DWP's Problems over the term of the Services;
  - xi. Change Management - a review of DWP's changes undertaken over the term of the Services; xii. supervised hands-on experience of operating the systems and processes, wherever possible, including monitoring and scheduling toolsets;
  - xiii. details of physical and logical security processes and tools which shall be available to DWP; and
  - xiv. any relevant interface information.

## 5. ACCESSIBILITY



## 5.1. Supplier Accessibility Testing

Previously, Digital Accessibility Compliance (DAC) team within DWP would allocate an Accessibility Compliance Manager to work with each project to help and advise projects on how to meet the legislation. That role has now been stood down. The responsibility for ensuring all systems are compliant with the legislation now sits with Application, Product and Business Owners.

## 5.2. Supplier Software Compliance

Accessibility Testing within DWP project (CCMP) means ensuring that the platform applications; WFM, Workspace, Softphone Workspace, Pulse, Verint, and GAX and GCXI are usable by all DWP staff, with particular focus on those who might otherwise be excluded for reasons of disability. However, not everyone with accessibility needs uses assistive software to access IT. This means it is necessary to ensure the NGCC applications are accessible to people who do not have the additional support provided by assistive software, so the first priority is to comply with the accessibility standards.

To determine that the applications are accessibility compliant they will be tested against one of the two standards mandated within DWP.

- WCAG v2.1 AA standard which can only be directly applied to web-based products and services.
- EN 301 549 which can be applied to a range of products including hardware and non-web applications, closed systems and documentation.

5.2.1. Testing websites to the WCAG v2.1 AA standard will also satisfy The Public Sector Bodies (Website and Mobile Application) Accessibility Regulations 2018 which require a website or mobile app to be more accessible by making it 'perceivable, operable, understandable and robust'.

5.2.2. The focus for DWP project (CCMP) is Accessibility Testing is to meet the WCAG v2.1 to AA

level standard, A completed DWP document DAC03 is required to support this. To achieve compliance all standards that are applicable to each application should be passed and appropriate evidence is required.

5.2.3. Testing the applications alone will not ensure compliance. Each application should also be tested using the four main types of assistive software; JAWS, Dragon, Zoomtext, Read & Write Gold. This will establish that, as well as meeting the acceptance criteria laid out in the standards, the product is also fully usable in a practical sense across the organisation.

5.2.4. Once the DWP project team has completed its own testing it, final testing will be undertaken using assistive software users from within DWP to do a final user test for usability.

5.2.5. It is expected that specialist testing resource will be brought on to the Programme to undertake the Accessibility compliance testing through DWP BAU support.

## 6. RESPONSIBILITIES OF DWP

DWP will provide:

- a) DWP will provide high-level design documentation to the Supplier.
- b) Relevant resource attendance at scheduled workshops.

- c) Information required for the Supplier to produce documentation.
- d) All relevant project documentation e.g. HLSO, Comms plan RAAIDD, RACI
- e) Relevant licences for access to third party systems.
- f) Provision of laptops where required to access DWP systems.

## **7. CHANGE MANAGEMENT**

Change Management will apply when there is a requirement from either party to deviate from the solution and delivery as described within the project governance documents. Any changes will be mutually agreed by both parties. At a high level the following principles will apply.

No verbal agreement between persons involved in the Project will be binding on either the Supplier or DWP.

Both the DWP and Supplier Project Managers will be the designated authorising representatives for requesting/accepting changes.

Typical stages for the Change Management process are:

### **Step 1 Project Change Recognition**

- Both parties agree on change details and that a Change Request is applicable

### **Step 2 Document Production**

- Establish control documentation around the Change Request

### **Step 3 - Analyse**

- Analyse Change and identify:
  - Impacts on solution and timelines
  - Reasoning and recommendations
  - Budgetary Impacts if applicable

### **Step 4 - Approval**

- Approval for the change will be authorised by the designated authorising representative of both parties.

### **Step 5 - Implementation**

- The implementation of the Change Request will be scheduled at a time that is mutually agreeable to both parties.
- Changes requiring a contract Variation will not come into effect until the Variation documentation is executed.

The Supplier is required to comply with all Buyer change freeze windows.

## **8. PLAN ACCELERATION**

- 8.1.** The Supplier shall work with the Buyer to seek opportunities to accelerate the delivery plan.
- 8.2.** Plan acceleration and optimisation activities are expected to be an ongoing task throughout the delivery of the Services.

- 8.3.** The Supplier shall arrange plan optimisation workshops with the CCMP team to explore opportunities to complete the implementation by March 2023.
- 8.4.** The Supplier shall ensure that plan optimisation and acceleration is a standing agenda item on the monthly review sessions and shall report on activities undertaken and progress made.
- 8.5.** Where there is a mutual agreement to change a milestone delivery date then this will be incorporated into the Call-Off Contract via the Variation process.

## **Annex 1 – Supplier Clarification Response**

The Supplier's clarification response is set out below

### **1. CLARIFICATION QUESTIONNAIRE RESPONSE**



CLARIFICATION  
RESPONSE.docx

### **2. PRICING RESPONSE**



Pricing Response

### **3. PROGRAMME PLAN**



Programme Plan

### **4. ASSUMPTIONS, DEPENDENCIES AND PRE-REQUISITES**



RAID.xlsx

### **5. BUYER Q&A RESPONSES**



Buyer Clarification  
Responses

### **6. SUPPLIER Q&A RESPONSES**



Supplier QA  
Response

## Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. All Charges are stated exclusive of VAT. The detailed Charges breakdown for the provision of Services during the Term will include:

### 1. IMPLEMENTATION CHARGES

- 1.1. The Supplier shall deliver the Services for a fixed price of £3,262,340 (excluding VAT) inclusive of all expenses.
- 1.2. The Supplier shall deliver the required milestones by the associated Milestone Completion Date.

[Redacted]

- 1.3. A Milestone will be considered complete when all associated deliverables have been completed in accordance with the stated acceptance criteria.
- 1.4. The detailed breakdown of the deliverables within each milestone can be found in section 2.1 of Schedule 1 Services.
- 1.5. Upon completion of a Milestone, the Supplier shall submit a milestone acceptance certificate (in the attached form). A milestone acceptance certificate will be required in respect of each milestone for formal certification prior to invoicing.



Milestone  
Certificate.docx

- 1.6. If the level of effort required from the Supplier to deliver the Services is subsequently understood to be materially less than originally forecasted then, by mutual agreement, the Parties may agree to reduce the charges by a proportional value. Such a change to be enacted by a mutually agreed Variation.

### 2. RATE CARD

- 2.1. The following day rates are to be used in calculating pricing for any Variations or subsequent Statements of Work. The pricing model for each Variation or Statement of Work (eg. fixed price, time and materials, risk/gain share or any other mechanism) will be defined within the Variation/Statement of Work and should be derived from the pricing in this section.
- 2.2. Day rates exclude VAT and expenses.
- 2.3. Any permissible expenses are to be charged in accordance with the Buyer's expense policy attached:



Expenses Policy.docx

2.4. The Supplier is required to provide transparency of any risk or contingency values within their Statement of Work or Variation pricing.

<b>DWP Role Description</b>	<b>SFIA Grade</b>	<b>Day Rate</b>
Programme Manager	6	£860.00
Project Manager	6	£860.00
Senior Project Manager	6	£860.00
Genesys Consultant (Potential Supplier)	6	£860.00
Genesys Consultant (Genesys)	6	£1,280.00
Verint Consultant (Potential Supplier)	6	£860.00
Verint Consultant (Verint)	6	£1,400.00
Infrastructure Consultant	6	£860.00
Business Consultant	6	£860.00
Architect	6	£860.00
DevOps	6	£860.00
Testing Manager	6	£860.00
Senior Tester	4	£690.00

## Part B: Terms and conditions

### 1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

## 2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

- 2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.
- 2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

### 4. Supplier staff

- 4.1 The Supplier Staff must:
  - 4.1.1 be appropriately experienced, qualified and trained to supply the Services
  - 4.1.2 apply all due skill, care and diligence in faithfully performing those duties
  - 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
  - 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
  - 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.



- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

## 5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
  - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
  - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
  - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
  - 5.1.4 have entered into the Call-Off Contract relying on its own due diligence

## 6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

## 7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

## 8. Recovery of sums due and right of set-off

- 8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

## 9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:
  - 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
  - 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
  - 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
  - 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of

£5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
- 9.4.1 a broker's verification of insurance
  - 9.4.2 receipts for the insurance premium
  - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
  - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
  - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
- 9.8.1 premiums, which it will pay promptly
  - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

## 10. Confidentiality

- 10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royaltyfree licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
  - 11.5.1 rights granted to the Buyer under this Call-Off Contract
  - 11.5.2 Supplier's performance of the Services
  - 11.5.3 use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
  - 11.6.1 modify the relevant part of the Services without reducing its functionality or performance
  - 11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - 11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.7 Clause 11.5 will not apply if the IPR Claim is from:
  - 11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.7.3 other material provided by the Buyer necessary for the Services
- 11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12. Protection of information

- 12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

### 13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:

<https://www.gov.uk/government/publications/government-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: <https://www.gov.uk/government/publications/technology-code-ofpractice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 buyer requirements in respect of AI ethical standards

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## 14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: <https://www.gov.uk/government/publications/technology-code-of-practice/technology-codeof-practice>

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15. Open source

- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
- 15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

## 16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
  - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
  - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

## 17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

## 18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

- 18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:



18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

## 19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

## 20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

## 21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
  - 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
  - 21.6.2 there will be no adverse impact on service continuity
  - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
  - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
  - 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
  - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

## 22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

## 23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

## 24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

## 25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

## 26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

## 27. The Contracts (Rights of Third Parties) Act 1999

- 27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

## 28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

## 29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
- 29.2.1 the activities they perform
  - 29.2.2 age
  - 29.2.3 start date
  - 29.2.4 place of work
  - 29.2.5 notice period
  - 29.2.6 redundancy payment entitlement
  - 29.2.7 salary, benefits and pension entitlements
  - 29.2.8 employment status
  - 29.2.9 identity of employer
  - 29.2.10 working arrangements
  - 29.2.11 outstanding liabilities
  - 29.2.12 sickness absence
  - 29.2.13 copies of all relevant employment contracts and related documents
  - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
- 29.6.1 its failure to comply with the provisions of this clause
  - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.
- 30. Additional G-Cloud services**
- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.
- 31. Collaboration**
- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
- 31.2.1 work proactively and in good faith with each of the Buyer's contractors
  - 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services
- 32. Variation process**
- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this CallOff Contract by giving 30 days notice to the Supplier.

### 33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

## Schedule 3: Collaboration agreement

Not required



## Schedule 4: Alternative clauses

### 1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

### 2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FOIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

### 2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003 □  
Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997

- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

- a. persons of different religious beliefs or political opinions
- b. men and women or married and unmarried persons
- c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
- d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
- e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
- f. persons of different ages
- g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

## 2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

- a. the issue of written instructions to staff and other relevant persons
- b. the appointment or designation of a senior manager with responsibility for equal opportunities
- c. training of all staff and other relevant persons in equal opportunities and harassment matters
- d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

- A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
- B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

## 2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

## 2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the CallOff Contract. The Customer will promptly notify the Supplier of any health and safety

hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

## 2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

## Schedule 5: Guarantee

Not required

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>• owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>• created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>

<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.

<b>Buyer Software</b>	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
<b>Call-Off Contract</b>	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.

<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
<b>Confidential Information</b>	Data, Personal Data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> <li>• information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the GDPR.
<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b>	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.



<b>Data Protection Legislation (DPL)</b>	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
<b>Data Subject</b>	Takes the meaning given in the GDPR
<b>Default</b>	Default is any: <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>Deliverable(s)</b>	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
<b>Digital Marketplace</b>	The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.

<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="https://www.gov.uk/guidance/check-employment-status-for-tax">https://www.gov.uk/guidance/check-employment-status-for-tax</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.

<p><b>Force Majeure</b></p>	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<p><b>Former Supplier</b></p>	<p>A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).</p>
<p><b>Framework Agreement</b></p>	<p>The clauses of framework agreement RM1557.12 together with the Framework Schedules.</p>
<p><b>Fraud</b></p>	<p>Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.</p>

<b>Freedom of Information Act or FoIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
<b>GDPR</b>	General Data Protection Regulation (Regulation (EU) 2016/679)
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.

<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency event</b>	<p>Can be:</p> <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand □ a Schedule A1 moratorium</li> </ul>

<b>Intellectual Property Rights or IPR</b>	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> <li>• copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</li> <li>• applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>
<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company <input type="checkbox"/></li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR claim</b>	<p>As set out in clause 11.5.</p>
<b>IR35</b>	<p>IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.</p>
<b>IR35 assessment</b>	<p>Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.</p>
<b>Know-How</b>	<p>All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.</p>

<b>Law</b>	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>LED</b>	Law Enforcement Directive (EU) 2016/680.
<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement section 6 (What you report to CCS).
<b>Material Breach</b>	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.

<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the GDPR.



<b>Processing</b>	Takes the meaning given in the GDPR.
<b>Processor</b>	Takes the meaning given in the GDPR.
<b>Prohibited act</b>	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical
	documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's highperformance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the CallOff Contract, whether those services are provided by the Buyer or a third party.
<b>Replacement supplier</b>	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service data</b>	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.

<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Digital Marketplace.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the GCloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.

<b>Supplier terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

## Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

### 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 Buyer at its absolute discretion.

1.1 The contact details of the Buyer's Data Protection Officer are: Dominic Hartley, data.protection@dpw.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: Legal Department, legals@sabiogroup.com

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.

Descriptions	Details
Identity of Controller for each Category of Personal Data	<p><b>The Parties are Independent Controllers of Personal Data</b></p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> <li>• Business contact details of Supplier Personnel for which the Supplier is the Controller</li> <li>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller</li> </ul>
Duration of the Processing	The duration of the call-off contract

Nature and purposes of the Processing	<p><b>Supplier Processing</b></p> <p>The Supplier is not engaged to Process Buyer Personal Data, however, the Supplier may (i) have the ability to access Buyer Personal Data by virtue of access to Buyer systems and/or (ii) receive Buyer Personal Data by virtue of correspondence between the Parties. In respect of (i), all such Buyer Personal Data will remain within the Buyer estate and the</p>
	<p>Buyer will remain responsible for all data handling controls. The Supplier will follow the Buyer's direction and guidelines on staff security clearance and processes for access to Buyer systems, including role-based access controls and security standards. Where the Supplier is required to grant user access, this will be undertaken at the Buyer's direction. Access for the Supplier to Buyer systems will be limited to Buyer provisioned laptops and approved USB devices. Any requirement to share data externally, such as with third parties for diagnostic purposes, is not to be undertaken by the Supplier and will remain the responsibility of the Buyer. In respect of (ii), the nature of the Processing by the Supplier shall be limited to the storage and retrieval of Buyer Personal Data as is necessary for the Supplier to contact and communicate with the Buyer in order to properly perform this Call Off Contract.</p> <p><b>Buyer Processing</b></p> <p>The nature of the Processing by the Buyer shall be for the recording, storage and retrieval of Supplier Staff business contact details and images. The purpose of such Processing by the Buyer is in order to receive the Services under this Call Off Contract and will include such Processing as is required in accordance with Buyer standard practice in order to permit access to Buyer data, information technology systems and premises.</p>
Type of Personal Data	Name, business e-mail address, business telephone number, and in respect of Supplier Staff image.

Categories of Data Subject	Any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) for which the Buyer is the Controller  Supplier Staff engaged in the performance of the Supplier's duties under the Contract for which the Supplier is the Controller.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Erase or destroy appropriately.

## Annex 2: Joint Controller Agreement

Not Applicable