Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

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.

Platform service ID number	638479524172955
Call-Off Contract reference	Project_25719.
Call-Off Contract title	Middleware and Software provided Session Border Controllers (eSBC) Support Service – DWP Contact Centre Test Automation
Call-Off Contract description	This requirement is for a new contract for the supply of a Support Service with Sabio Ltd which will be awarded using CCS framework G-Cloud 13 for one year. This Service is required for Contact Centre Test Automation an integral part of DWP's Contact Centre Infrastructure. Currently there is a gap in support for both the Middleware and virtual Session Border Controllers (eSBC) that form part of the infrastructure required to deliver DWP's Test Automation services. The future plan is to perform these support services "in house" but in the interim and before this transition is possible a third-party support solution is required to protect and maintain service.
Start date	28 March 2023
Expiry date	27 March 2024
Call-Off Contract value	£72,650.00 (excluding VAT)
Charging method	The maximum Call-Off Contract value of the 1-year initial term is £72,650.00 (excluding VAT) and is a fixed price for services, paid in advance
Purchase order number	39070260383

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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 Services 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.

From the Buyer	Department for Work and Pensions DWP Commercial Directorate Finance Group 5th Floor 2 St Peter's Square Manchester M2 3AA
To the Supplier	Sabio Ltd +44(0)344 412 3000 London – Head office 12th Floor, Blue Fin Building 110 Southwark St. London UK SE1 0SU Company number: 03644452
Together the 'Parties'	

Principal contact details

For the Buyer:

[REDACTED]

For the Supplier:

[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 28 March 2023 and is valid for 12 months.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is **30** days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for two separate one-year periods which run would consecutively. If both one-year extensions were exercised by the Buyer, the contract would end in entirety no later than 27 March 2026. For any extension period the Buyer would need to gain addition expenditure approval via the Buyers Commercial governance process, and the price for any extension period will be subject to agreement between the Supplier and the Buyer, with any increase in the Suppliers price being capped at 5% per year. The Buyer needs to provide 8 weeks written notice to extend the contract before its expiry date. The extension period is subject to clauses 1.3 and 1.4 in Part B below.

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.

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: ● Support for Middleware and eSBC’s infrastructure and

	Software required for DWP's Test Automation Services
Additional Services	Additional Services are not applicable to this Call-Off Contract unless this Call-Off Contract is subsequently varied post the Start Date through the Variation process set out in clause 32 of this Call-Off Contract
Location	The Services shall be delivered remotely unless there is specific issue that requires on site presence at the Buyers locations. If the Supplier is required to attend the Buyers locations, then travel and subsistence expenses will be paid in line with the Buyers travel and subsistence policy.
Quality Standards	The quality standards required for this Call-Off Contract are as per the G-Cloud framework standards and ISO27001.
Technical Standards:	Technical requirements are set out in Schedule 1 – Services.
Service level agreement:	The service levels and associated service credits required for this Call-Off Contract are stated below in Schedule 1 – Services.
Onboarding	The on boarding plan for this Call-Off Contract is as stated in Schedule 1 - Services.

Offboarding	To the extent required and applicable, offboarding requirements shall be defined in each Statement of Work. Offboarding requirements may include but not be limited to: • All artefacts/data relating to the scope of Services (Schedule 1) will be handed over to the Buyer at the time of off-boarding without any cost implications or IPR restriction (subject to Clause 11). • Deletion of Buyer data. • Knowledge transfer. • At the end of the off-boarding and handover period - removal of security clearance and site/system access for the Supplier by the Buyer.
Collaboration agreement	N/A
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed **[REDACTED]** The annual total liability for Buyer Data Defaults will not exceed **[REDACTED]** or [**REDACTED]** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). Clause 24.1 in Part B below applies for a more in-depth definition of Buyer Data Defaults, while still maintaining the definitions and meanings of Buyer Data and Default in Schedule 6: Glossary and Interpretations below. The annual total liability for all other Defaults will not exceed **[REDACTED]** of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. Clause 24.1 in Part B below provides a definition of Other Defaults.

Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● 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 **[REDACTED]** for each individual claim or any higher limit the Buyer requires (and as required by Law) employers' liability insurance with a minimum limit of **[REDACTED]** or any higher minimum limit required by Law

Buyer's responsibilities	• The Buyer will provide suitable access to the environment in a manner which will not restrict The Supplier from providing the support services.
	• Service restoration targets are indicative and subject to Buyer support activities and processes. Any delays on the Buyer side in accepting, reviewing approving changes for support purposes will stop the service target clock.
	• The Buyer is responsible for security vulnerability monitoring, assessments and management, including highlighting to the Supplier vulnerabilities applicable to the Test Orchestration Middleware solution.
	• The following exclusions, caveats & assumptions apply to the performance of Adaptive Maintenance:
	  • The Buyer shall be responsible for providing notice of upgrades, updates and changes to the underpinning solution components and inform the Supplier in a timely manner (minimum 14 days' notice).
	  • The Buyer shall provide access to a suitable test environment to allow the development and testing of required adaptations of the Test Orchestration Middleware solution.
	  • The Buyer will support testing where necessary to sign-off the adaptations the Test Orchestration Middleware solution.
	• The provision of a suitable Oracle eSBC vendor support service (for software patches and release updates) is the responsibility of the Buyer.

Buyer's equipment	• The Buyer will provision sufficient Buyer devices for the Supplier support teams to obtain access to the Buyers solution environment (approximately 5 devices)

Supplier's information

Subcontractors or partners	No Subcontractors or Partners and used by the Supplier to deliver this service

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.

Payment method	**[REDACTED]**
Payment profile	The payment profile for this Call-Off Contract is set out in Schedule 2
Invoice details	The Supplier will post paper invoices 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. 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. The Buyer will pay the Supplier within 30 days of receipt of the valid PDF invoice at SSCL.
Who and where to send invoices to	Hard copies and electronic invoices shall be sent and emailed respectively to: **[REDACTED]**

Invoice information required	All invoices must include purchase order number, contract reference and Buyer's reference details. 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. 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.
Invoice frequency	Invoices for services will be sent to the Buyer in advance of Service commencement.
Call-Off Contract value	The total value of this Call-Off Contract is set out in the Call-Off Contract section in Part A of the Order Form.
Call-Off Contract charges	The breakdown of charges are the agreed Charges set out in the Payment Profile in Schedule 2. Where Supplier expenses are applicable, they must be agreed in advance with the buyer and will charged in accordance with the Buyer's expense policy as attached in Schedule 2.

Additional Buyer terms

Performance of the Service	As per Schedule 1 and any agreed Variations.
Guarantee	Not Applicable
Warranties, representations	No additional warranties to those incorporated in the Framework agreement clause 2.3, are required.

Supplemental requirements in addition to the Call-Off terms	**"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. 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. **3.Risk Management** 3.1 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.

3.2 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.

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

3.4 **[REDACTED]**

4. 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.

5. Security Tests

5.1 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.

5.2 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.

5.3 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.

6. 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.

7. Security Policies and Standards

7.1 The Supplier shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Buyer Security Policies and Standards set out below.

7.2 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. Buyer Security Policies and Standards

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-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-personnel-security-controls)
p) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

9. Cyber Security Information Sharing Partnership

9.1 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.

9.2 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.

10. Security Clearance

Security clearance requirements are to be identified as required.

11. Not used

	12. Offshoring The Supplier has confirmed that the Services do not fall within the definition of Offshoring as stated in the Buyer's Offshoring Policy. **13. Prohibited Acts** The Supplier shall not, and shall ensure that any staff shall not, commit any Prohibited Act. If the Supplier, its staff or anyone acting on the Supplier's behalf engages in a Prohibited Act, the Buyer may terminate the Call-Off Contract and recover from the Supplier the amount of any Loss suffered by the Buyer as a result. Any termination under this clause of the Call-Off Contract will be without prejudice to any right or remedy which has already accrued or subsequently accrues to the Buyer. **14. Not used** **15. Social Value** The Supplier shall provide a monthly update at governance review meetings on the steps the Supplier is taking to ensure delivery of this Call-Off Contract supports the Buyer's theme of "Equal Opportunities" with the required policy outcome being "Tackle workforce inequality".
Alternative clauses	None required
Buyer specific amendments to/refinements of the Call-Off Contract terms	None required
Personal Data and Data Subjects	See Annex 1 below

Intellectual Property	The parties agree that clauses 11.3 and 11.4 shall be amended as follows: 11.3 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. 11.3.1 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. 11.4 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.
Social Value	No applicable Social Value within this call off

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call Off 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 RM1557.13 .

Signed	**Supplier**	Buyer
Name	[REDACTED}	[REDACTED}
Title	[REDACTED}	[REDACTED}
Signature	[REDACTED}	[REDACTED]
Date	24th March 2023	27th March 2023

2.2 The Buyer provided an Order Form for Services to the Supplier.

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record

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 12 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 period of up to 12 months.

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 set the Term at more than 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:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)

- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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' or to 'CCS and/or the Buyer' 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 7 (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 their 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 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 incorporated Framework Agreement clause 34. 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 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer 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:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 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:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 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

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, 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-securityclassifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.cpni.gov.uk/content/adopt-risk-managementapproach 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/technologycode-of-practice/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-code-of-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. 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 are reasonable compensation and cover 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); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (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 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30-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 take the Term beyond 36 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 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 30 consecutive days, 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 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per

cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

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

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.

29.3 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.

29.4 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.

29.5 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.5.1 its failure to comply with the provisions of this clause

29.5.2 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

29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.7 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 Call Off 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, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

Detailed below in Sections **A** and **B** are the Buyer requirements for the G-Cloud Services that the Suppliers Service needs to deliver.

Detailed below in Sections **C** is the Supplier Service that meets and delivers the Buyers requirements as detailed in Sections **A** and **B** and which has been agreed by both the Buyer and the Supplier.

In the event of any conflict or inconsistency between the sections of this schedule, Section C shall take precedence.

Buyers Service Requirements for Middleware Tool Support and eSBC Support the Contact Centre Test Automation Service

A. Buyers Requirements for Services to support the Middleware Tool for the Contact Centre Test Automation Service

1. In Scope

1.1 Standard Support Mon-Fri 8-6
1.2 Bug Fixes / Service affecting issues
1.3 Integration with Zephyr, Nectar, & TestComplete
1.4 Middleware code / Middleware Integrations / Environment / infrastructure support (e.g. re-starting services
1.5 Security/vulnerability issues (arising from routine patching & upgrades)

2. Service Level Agreement Severities 1 to 3 (P1 to P3)

Severity 1 (P1)

2.1 Application not responding
2.2 Unable to access application
2.3 All transactions not processed

Severity 2 (P2)

2.2 Individual process not running as expected
2.3 API integration issues
2.4 Vulnerability issues
2.5 Incorrect states being returned

Severity 3 (P3)

2.6 Patching issues
2.7 Maintenance tasks

B. Buyer Requirements for eSBC Support for the Contact Centre Test Automation Service

3. In Scope

3.1 Fault diagnosis & restore
3.2 Retrieve Logs
3.3 Wireshark tracing
3.4 Configuration changes (add & remove number ranges, rules etc)
3.6 Security patching
3.7 Update patching
3.8 Vulnerability analysis
3.9 Business Hours Mon-Fri 8-6

4. Service Level Agreement Severities 1 to 3

Severity 1 (P1)

4.1 Calls not being made
4.2 Call features not working
4.3 Integration to Media Server / Gamma not working

Severity 2 (P2)

4.4 Call concurrency issues
4.5 API integration issues
4.6 Vulnerability issues

Severity 3 (P3)

4.7 Patching issues
4.8 Maintenance tasks
4.9 Configuration changes to support new ways of working

5. For both Middleware and eSBC the following Buyer requirements apply to both needs.

5.1 KPI's – to support SLA's
5.2 Escalation path and invocation times
5.3 Process for raising tickets
5.4 Monthly performance report / service review

C. The agreed Suppliers Service and Support Solution for the Buyers Middleware Tool and eSBC service needs for Contact Centre Test Automation is detailed as follows:

Suppliers Service Solution

The DWP Test Orchestration (TO) solution is built around three core applications integrations: Nectar, Zephyr and Test Complete. A bespoke test orchestration middleware application has been developed by The Supplier to provide an orchestration process across the three core applications allowing the solution to provide the automated test executions.

The Supplier is providing an application support service for the Test Orchestration Middleware solution including support for the integration points (APIs) within the current solution LLD defined in the solution status below. In addition, The Supplier will be providing support services for the Oracle e-SBC which forms part of the Test Orchestration Middleware solution .

The Test Orchestration Middleware solution is made up of the following elements:

Solution Element	Description	Responsibility
Connectivity Services	Connectivity and network service	The Buyer
Infrastructure Services	The server compute, operating system and database services provision, management and support	The Buyer
Test Orchestration Middleware Application	The Middleware solution developed in Go programming language	The Supplier

Containerisation Solution	Podman Containerisation solution	The Supplier
Nectar	A The Buyer provisioned third party CX assurance service test orchestration service	The Buyer
TestComplete	A The Buyer provisioned third party test orchestration service	The Buyer
Zephyr	A The Buyer provisioned services to provide test orchestration results	The Buyer
Oracle e-SBC	The single virtual oracle session border controller deployed within the pre-production environment	The Supplier

Solution Status

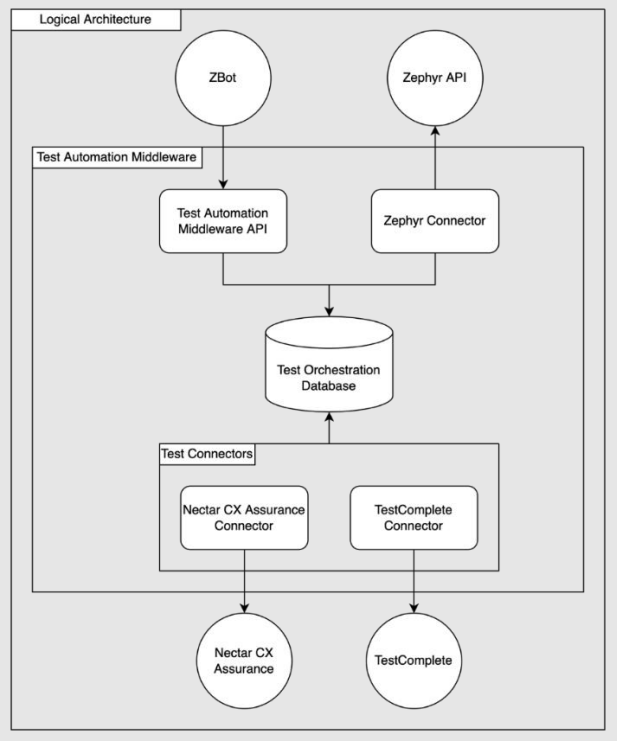
This is an active solution, and the source of truth for the design of the solution can be found in the High & Low-Level Design Documents (LLD).

- CCMP Test Automation Middleware LLD
- CCMP eSBC LLD
- NGCC Test Automation Middleware High Level Design

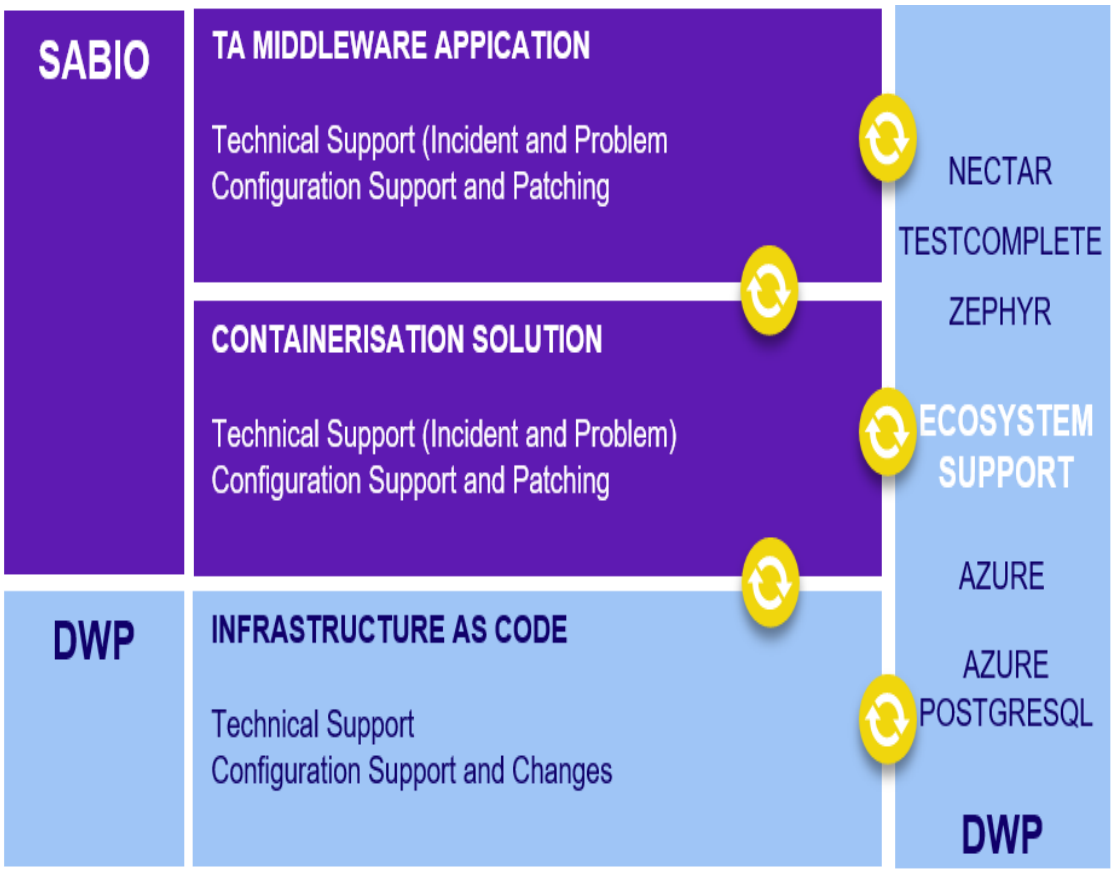
Furthermore, the source code of the Test Orchestration Middleware Solution is stored in the Buyer Gitlab repository. The Buyer is responsible for source code management including backups and restores to the known good version of the software.

The Buyers Test Orchestration Middleware solution is deployed into a pre-production environment which will be co-supported between the Buyer's support and operations teams and The Supplier support teams.

The diagram below provides the overview of the logical architecture of the Test Orchestration Middleware solution elements and integrations.



The following diagram provide a conceptual deployment of the solution elements and who is responsible for the solution element. Support will be provided collaboratively between The Supplier teams, and the Buyer support teams to minimise the risk of gaps in the service boundaries.



Scope of Service

Incident Management

The Supplier will provide incident support via our Global Service Centre. The Buyer will be able to raise tickets The Supplier via the Service Management Portal, combined with a telephone call for priority 1 incidents.

- [REDACTED]
- [REDACTED]

The Supplier technical support resources working on the Buyer's solution will use devices (laptop or equivalent technology) provided by the Buyer and The Supplier support resources will be based in the UK. The Supplier will provide the Buyer with the details of the Supplier technical resources who require a laptop or equivalent technology.

Support hours are detailed in the coverage hours section. Service target response and resolution times are defined within the service level section.

The Buyer shall provide the Supplier with a nominated single of contact (email mailbox and escalation contact details) where issues need to be communicated to and investigated with the Buyer's support teams.

This service applies to the Test Orchestration Middleware Application, Containerisation Solution and Oracle e-SBC application.

Problem Management

Where the Test Orchestration application requires a bugfix to restore service, these fixes are included within the scope of the services, to the extent that the problem is not chargeable change (See Change Management).

The Supplier has included an adaptive maintenance service (see Adaptive Maintenance) to support configuration changes of the supported solution where changes to the solution ecosystem require standard configuration activities to enable the Test Orchestration Middleware solution to remain operational. Where there is a complex change or new requirements needed within the Test Orchestration Middleware solution ecosystem, such changes will follow the commercial change process to impact assess the scope of the change.

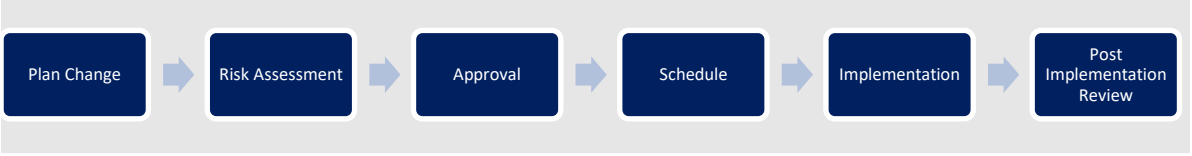
This service applies to the Test Orchestration Middleware Application, Containerisation Solution and Oracle e-SBC application.

Change Management

All requests for configuration adaptions or change requests shall be logged via the Supplier Service Portal as a service request.

Operational changes will be delivered via the Supplier change management process which will ensure changes are governed correctly to minimise risk to the solution delivery.

The Supplier Change management process follows 6 steps:



Chargeable Changes

Chargeable changes are those changes which are requested/required and impact the scope of the services support delivery (i.e., enhanced service hours, variation to service levels) and/or where the current deployed Test Orchestration Middleware solution needs to be enhanced or expanded with more instances, new features and/or functionality or where major upgrades to the solution are needed to maintain the existing functionality i.e. a 1.x.x software update.

Changes which are deemed to be chargeable will be discussed with the Buyer and The Supplier Account Manager, and where applicable a change advisory notice/change request form will be raised by the Buyer to define the impact of the change. Where The Supplier identify a change requirement, a change advisory notice/change request will be raised and be sent to the Buyer.

This service applies to the Test Orchestration Middleware Application, Containerisation Solution and Oracle e-SBC application.

Security/Vulnerability Patching

The Buyer will undertake vulnerability assessments and report to The Supplier any issues which arise from the assessment. The Buyer will categorise the security vulnerabilities in accordance with the CVSS 3.1 score and The Buyer severity of impact i.e., critical, high, medium, low, none.

The Supplier will provide remediation plans in conjunction with the Buyer for high and critical vulnerabilities on an ad-hoc basis. For medium vulnerabilities plans will be reviewed monthly and patched no later than quarterly, for low vulnerabilities such plans will be reviewed quarterly and patched no later than on a 6 monthly basis in-line with the time frames below.

The remediation activity shall be carried out in-line within these time frames below.

- Critical = [REDACTED]
- High = [REDACTE]
- Medium = [REDACTED]
- Low = [REDACTED]

Where a suitable remediation is not available i.e., the security patch is not available from a vendor, such issues will be reported to the Buyer nominated service owner for onward management within the Buyer organisation. The incident ticket service level clock will be paused until such time as an applicable remediation can be completed.

Where a configuration change is required to resolve the vulnerability within the Test Orchestration Middleware solution this will be carried out using the Adaptive Maintenance service. Where the vulnerability requires a significant development change i.e., a major software version release 1.x.x, such occurrences will be scoped and quoted as part of the chargeable change as defined in the change section above.

The Supplier will report to the Buyer, those vulnerabilities reported within the Test Orchestration Middleware solution which have been identified as related to the underpinning solution, i.e. are inherited from the Buyer's gold build and require onward management by the Buyer to resolve.

The Supplier nominated representative will interface with the Buyer nominated service owner and/or nominated representative to discuss vulnerabilities and remediation plans.

This service applies to the Test Orchestration Middleware Application, Containerisation Solution and Oracle e-SBC application.

Adaptive Maintenance Service

The Supplier shall provide an Adaptive Maintenance service which will provide configuration adaptations (i.e. no major development to the core code and/or agreed solution functionality/features) to the supported Test Orchestration Middleware solution elements (Application and Container), this is to ensure the Test Orchestration Middleware solution continues to operate to the agreed functionality and configuration, as defined within design documents and source code following a minor change, update or upgrade to the underpinning solution components, that otherwise would prevent the Test Orchestration Middleware application from operating to the agreed designs.

Configuration Adaptations can include but are not limited to supporting changes i.e., minor Test Orchestration Middleware solution adaptations to resolve vulnerabilities, IP address changes, service naming changes, Azure resource groups, integration system passwords and certificates.

All configuration requests or change requests shall be logged via the Supplier Service Portal.

Where changes are jointly assessed between the Buyer and The Supplier and are agreed to be out of scope of a configuration adaptation they will be raised as a change advisory notice/change request for review as a chargeable change (see Chargeable Changes definition).

The Supplier's Adaptive Maintenance activities will be undertaken via change management to ensure suitable controls are in place to agree the scope of the required adaptations and to ensure that adaptations are first deployed and tested within a The Buyer's development environment (where available) prior to deployment in the Buyer's test environment.

The Supplier and the Buyer will agree on a case-by-case basis how the required adaptations are prioritised, delivered and the applicable fulfilment timelines.

For changes to the Test Orchestration Middleware solution ecosystem and underpinning solutions i.e. the integrated systems and Infrastructure gold build changes which are outside of The Supplier control, The Supplier expect a minimum of 14 days' notice from the Buyer for any changes to be assessed and impact provided i.e. Adaptive maintenance to fulfil a change or a commercial change request to be provide for additional development activities. Such notifications shall be made by the Buyer to the Account Manager for onward management.

This service applies to the Test Orchestration Middleware Application, Containerisation Solution only.

Vendor Support and Escalation

This service applies to the Oracle e-SBC application only.

The Buyer contracts Oracle directly for vendor support services, as such the Buyer will be responsible for providing support escalations to the vendor where The Supplier support teams have provided investigations and determine the issues needs to be reported to the Vendor. The Supplier will pause the SLA clock at this point, and the incident will be owned by the Buyer's support team until further The Buyer information and advice is provided.

The Buyer will be responsible for providing access to/providing the latest patch files applicable to The Supplier to provide the support services for this contract. For example, provision of security patches needed to resolve vulnerabilities, patches to resolve bug fixes. Applicable service levels will be put on hold whilst the relevant files are provided by the Buyer. The Supplier technical support teams will, in conjunction with the Buyer support teams and Vendor, confirm which patches are required from the vendor. The Buyer support teams will be responsible for requesting these from the Vendor.

Incident service levels align to the incident management section of this document.

Security patching for vulnerabilities will align with the targets defined within the security/vulnerability patching section of this document.

Coverage Hours

UK Normal Business Hours – Monday to Friday 08:00 – 18:00 excluding public and bank holidays.

Service Levels

Test Orchestration Middleware solution and Oracle eSBC

Target Response time

- P1 – [REDACTED]
- P2 – [REDACTED]
- P3 – [REDACTED]
- P4 – [REDACTED]

All new tickets logged via the portal will send out a “New Case” email to the Buyer nominated representative mailbox.

Target Restoration time

- P1 – [REDACTED]
- P2 – [REDACTED]
- P3 – [REDACTED]
- P4 – [REDACTED

*Where the investigations identify the need to make a configuration change to the Test Orchestration Middleware solution.

Where the investigations determine a chargeable change, The Supplier Account Manager will work with the Buyer to define the scope of the change advisory notice.

Definitions

Response means an acknowledgement of an issue reported to The Supplier, and which provides an indication that the fault is under review by a technical representative of The Supplier.

Restoration means the restoration of the supported solutions (or the relevant part thereof) to good working order (which may or may not mean that the root cause of the fault has been removed), which may be either a temporary or permanent fix or an agreed workaround which restores the supported solutions to an acceptable level.

Priority	Incident Characteristics
P1-Critical	Disruption in service is continuous or near continuous. No workaround is available. Emergency critical vulnerability^ Calls not being made. Call features not working. Integration to Media Server / Gamma not working.
P2-High	A significant proportion of core business functionality is degraded. However, some business function is still possible. No workaround is available. Critical and high vulnerabilities^ Call concurrency issues. API integration issues.
P3-Medium	Core business functionality is possible however ancillary business processes are degraded. No disruption to core business service. An ancillary business function is completely inoperative. An ancillary business function is disrupted continuously or near continuously. Medium vulnerability^
P4-Low	Core business functionality is possible however ancillary business processes are degraded. No disruption to core business service. An ancillary business function is degraded however some functionality is available. An ancillary business function is disrupted intermittently. Low Vulnerability^

^Security vulnerabilities which have been identified as security incidents will be prioritised and actioned in-line with the vulnerability remediation targets in the security/vulnerability patching section above. In the case where a critical vulnerability impact is severe, the Buyer and the Supplier can mutually agree to take emergency action in the review and remediation if necessary to the delivery of the Test Orchestration Middleware solution.

Support Procedures and Contacts

Service tickets can be raised by the Buyers nominated contacts to The Supplier's service centre by nominated The Buyer resources.

The Buyer shall provide the names and contact details of those nominated resources to the Supplier Account Manager.

Commercial change requests can be raised by the Buyer nominated approvers to the Supplier Account Manager.

Escalation Process

Incident escalations can be raised to the Supplier Service Centre.

Service performance issues shall be raised to the Service Centre and if required also escalated to your The Supplier Account Manager.

Service Management & Reporting

The Buyer will be able to track service tickets using the Supplier Service management portal

- [REDACTED]

- The Supplier will provide through the assigned service representative a monthly report. The reporting structure is as follows:
- Weekly (if required)
- Incident review meeting, attended by the Supplier service representative to discuss any major issues.
- Monthly
- SLA, Incident reporting, updates on Service Improvement Plans, Planned maintenance and patching services.

Service reviews will review the service reports and discuss the performance of the Supplier services in addition to any pertinent service topics agreed in advance, between the Supplier service representative and the Buyer nominated representatives.

Service reviews will be carried out remotely.

Supplier Caveats and Assumptions

- The Buyer will provision sufficient of the Buyer devices for the Suppliers support teams to obtain access to the Buyer solution environment (approximately 5 devices)
- The Buyer will provide suitable access to the environment in a manner which will not restrict The Supplier from providing the support services.
- Service restoration targets are indicative and subject to The Buyer support activities and processes. Any delays on the Buyer side in accepting, reviewing approving changes for support purposes will stop the service target clock.
- Development changes to the Test Orchestration Middleware solution will be chargeable activity and managed via change control.
- There are no service penalties associated with this service.
- The Buyer is responsible for security vulnerability monitoring, assessments and management, including highlighting to the Supplier vulnerabilities applicable to the Test Orchestration Middleware solution.
- The Supplier assumed they will not require regular attendance at the Buyers CAB meetings or similar forums where changes do not impact the Suppliers supported systems.
- The following exclusions, caveats & assumptions apply to the performance of Adaptive Maintenance:
    - The Buyer shall be responsible for providing notice of upgrades, updates and changes to the underpinning solution components and inform The Supplier in a timely manner **[REDATED]**
    - Adaptations to the Test Orchestration Middleware solution required as a result of upgrades, updates or changes to the underpinning solution which concern a major redevelopment of the Middleware application or introduce new features or functionality are not included within the scope of the Adaptive Maintenance service, such adaptations will be performed subject to Contract Change Control and will be separately chargeable.
    - The Buyer shall provide access to a suitable test environment to allow the development and testing of required adaptations of the Test Orchestration Middleware solution.
    - The Buyer will support testing where necessary to sign-off the adaptations the Test Orchestration Middleware solution.
- The Suppliers project delivery teams will be responsible for remediating the critical, high and medium graded vulnerabilities before the service is accepted into both the Buyer's and the Supplier's support teams.
- The provision of a suitable Oracle SBC vendor support service (for software patches and release updates) is the responsibility of the Buyer.

- The assumption is the SBC is deployed with suitable security hardening configuration to an agreed The Buyer security standard. Any changes to the security hardening will be assessed as a chargeable change.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the initial 12 month term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

1. Charges for the Service which total £72,650 excluding VAT [REDACTED]

Schedule 3: Collaboration agreement – Not Used

Schedule 4: Alternative clauses – Not Used

Schedule 5: Guarantee – Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	For each Party, IPRs: ● 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 ● created by the Party independently of this Call-Off Contract, or 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.

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

Buyer Software	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.
Call-Off Contract	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.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	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.
Commercially Sensitive Information	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.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: ● 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 ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	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.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR

Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● 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 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.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	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.
Equipment	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.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	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: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● 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 ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● 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
Former Supplier	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).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.

Fraud	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.
Freedom of Information Act or FoIA	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.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) 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.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	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.

Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	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.
Implementation Plan	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.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● 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 ● 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 ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the Supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a Buyer through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	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 Buyer through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	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 Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, 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.
Loss	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 '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	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.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	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.
Ministry of Justice Code	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.

New Fair Deal	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.

Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the UK GDPR.

Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	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: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	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.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	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.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	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.

Relevant person	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.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	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 Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	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).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.
Service definition(s)	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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	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.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.

Subcontract	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.
Subcontractor	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.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	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.
Supplier Terms	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.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

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: **[REDACTED]**

1.2 The contact details of the Supplier's Data Protection Officer are: **[REDACTED]**

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

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

Description	**Details**
Identity of Controller for each Category of Personal Data	The Parties acknowledge that they are Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Personnel for which the Supplier is the Controller ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller
Duration of the Processing	The duration of the Call-Off Contract

Nature and purposes of the Processing	**Supplier Processing** 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 visibility 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 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. 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. **Buyer Processing** 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.
Type of Personal Data	Name, business e-mail address, business telephone number, and 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	Erase or destroy appropriately.

Member State law to preserve that type of data	

Annex 2: Joint Controller Agreement

This Annex is not used