

# G-Cloud 11 Call-Off Contract (version 4)

**Contents**

[**G-Cloud 11 Call-Off Contract (version 4)** 1](#_Toc12278062)

[**Part A - Order Form** 3](#_Toc12278063)

[Principle contact details 4](#_Toc12278064)

[Call-Off Contract term 4](#_Toc12278065)

[Buyer contractual details 4](#_Toc12278066)

[Supplier’s information 6](#_Toc12278067)

[Call-Off Contract charges and payment 6](#_Toc12278068)

[Additional Buyer terms 6](#_Toc12278069)

[**Schedule 1 - Services** 17](#_Toc12278070)

[**Schedule 2 - Call-Off Contract charges** 33](#_Toc12278071)

[**Part B - Terms and conditions** 34](#_Toc12278072)

[1. Call-Off Contract start date and length 34](#_Toc12278073)

[2. Incorporation of terms 34](#_Toc12278074)

[3. Supply of services 35](#_Toc12278075)

[4. Supplier staff 36](#_Toc12278076)

[5. Due diligence 36](#_Toc12278077)

[6. Business continuity and disaster recovery 37](#_Toc12278078)

[7. Payment, VAT and Call-Off Contract charges 37](#_Toc12278079)

[8. Recovery of sums due and right of set-off 38](#_Toc12278080)

[9. Insurance 38](#_Toc12278081)

[10. Confidentiality 39](#_Toc12278082)

[11. Intellectual Property Rights 40](#_Toc12278083)

[12. Protection of information 41](#_Toc12278084)

[13. Buyer data 41](#_Toc12278085)

[14. Standards and quality 42](#_Toc12278086)

[15. Open source 43](#_Toc12278087)

[16. Security 43](#_Toc12278088)

[17. Guarantee 44](#_Toc12278089)

[18. Ending the Call-Off Contract 44](#_Toc12278090)

[19. Consequences of suspension, ending and expiry 45](#_Toc12278091)

[20. Notices 47](#_Toc12278092)

[21. Exit plan 47](#_Toc12278093)

[22. Handover to replacement supplier 48](#_Toc12278094)

[23. Force majeure 49](#_Toc12278095)

[24. Liability 49](#_Toc12278096)

[25. Premises 49](#_Toc12278097)

[26. Equipment 50](#_Toc12278098)

[27. The Contracts (Rights of Third Parties) Act 1999 50](#_Toc12278099)

[28. Environmental requirements 50](#_Toc12278100)

[29. The Employment Regulations (TUPE) 50](#_Toc12278101)

[30. Additional G-Cloud services 52](#_Toc12278102)

[31. Collaboration 52](#_Toc12278103)

[32. Variation process 52](#_Toc12278104)

[33. Data Protection Legislation (GDPR) 53](#_Toc12278105)

[**Schedule 3 - Collaboration agreement – not used** 53](#_Toc12278106)

[**Schedule 4 - Alternative clauses - not used** 53](#_Toc12278131)

[**Schedule 5 – Guarantee – not used** 53](#_Toc12278139)

[**Schedule 6 - Glossary and interpretations** 54](#_Toc12278152)

[**Schedule 7 - GDPR Information** 62](#_Toc12278153)

[**Annex 1 - Processing Personal Data** 62](#_Toc12278154)

## **Part A - Order Form**

|  |  |
| --- | --- |
| **Digital Marketplace service ID number:** | 3473 6819 3778 742 |
| **Call-Off Contract reference:** | SR339165068 COREDAS |
| **Call-Off Contract title:** | Bureau van Dijk Data Analysis Service – TP Catalyst |
| **Call-Off Contract description:** | A combination of comprehensive and detailed company information with flexible software including use of the Portal only.  |
| **Start date:**  | 31/03/2020 |
| **Expiry date:** | 30/03/2022 |
| **Call-Off Contract value:** | 2020: £200,0002021: £200,000 |
| **Charging method:** | Annual Invoice |
| **Purchase order number:** | TBC |

This Order Form is issued under the G-Cloud 11 Framework Agreement (RM1557.11).

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

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

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

|  |  |
| --- | --- |
| **From: the Buyer** | HM Revenue & Customs |
| **To: the Supplier** | Bureau van Dijk |
| **Together: the ‘Parties’** |

### Principle contact details

|  |  |
| --- | --- |
| **For the Buyer:** | Title: Senior Commercial Manager |
| **For the Supplier:** | Title: Account Director |

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date:** | This Call-Off Contract Starts on 31st March 2020 and is valid for 24 months.  |
| **Ending (termination):**  | The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.  |
| **Extension period:** | Not used |

### 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 2 – Cloud Software |
| **G-Cloud services required:** | The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:* Enterprise subscription for “TP Catalyst” company information and business intelligence
* Onsite and online training for portal users
* Helpdesk
 |
| **Additional Services:** | None |
| **Location:** | The Services will be delivered to all HMRC registered system users who may access these via desktop or remotely using secure portable IT devices. |
| **Quality standards:** | Any quality standards, where applicable, are outlined on the product description page on the Digital Marketplace and Schedule 1 below.  |
| **Technical standards:**  | Any technical standards, where applicable, are outlined on the product description page on the Digital Marketplace and Schedule 1 below. |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are outlined on the product description page on the Digital Marketplace and Schedule 1 below.  |
| **Onboarding:**  | The onboarding plan for this Call-Off Contract is training provided by Supplier, via its Customer Success team based in the UK. Onsite and online training will be rolled out as specified in Schedule 1 below. The Buyer may also access online video tutorials built within the solution.  |
| **Offboarding:**  | Not used |
| **Collaboration agreement:** | Not used |
| **Limit on Parties’ liability:** | The annual total liability of either Party for all Property defaults will not exceed £ 1,000,000. The annual total liability for Buyer Data defaults will not exceed £ 500,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).The annual total liability for all other defaults will not exceed the greater of £ 500,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). |
| **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 £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)
* employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
 |
| **Force majeure:** | A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days. |
| **Audit:** | As per Framework Agreement |
| **Buyer’s responsibilities:** | The Buyer is responsible for providing appropriate access to personnel. To include coordination of training requirement. |
| **Buyer’s equipment:** | Not used. |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners:** | Not applicable. |

### 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:** | The payment method for this Call-Off Contract is BACS. |
| **Payment profile:** | The payment profile for this Call-Off Contract is annually in advance. |
| **Invoice details:** | The Supplier will issue one electronic invoice for the full contract value each year. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice. |
| **Who and where to send invoices to:** | Invoices will be processed within the Ariba Network. |
| **Invoice information required** – for example purchase order, project reference: | All invoices must include Purchase Order number. |
| **Invoice frequency:** | Invoice will be sent to the Buyer once per year. |
| **Call-Off Contract value:** | The total value of this Call-Off Contract is £400,000. |
| **Call-Off Contract charges:** | The breakdown of the Charges is: TP CatalystYear 1: £200,000Year 2: £200,000 |

### Additional Buyer terms

|  |  |
| --- | --- |
| **Performance of the service and deliverables:**  | Not used |
| **Guarantee:** | Not used |
| **Warranties, representations:**  | Not used |
| **Supplemental requirements in addition to the Call-Off terms:** | BvD will disable company IDs on the administration site so that HMRC queries on the portal are anonymised to both parties.HMRC users will be able to access their own saved searches.**AUTHORITY’S MANDATORY TERMS**1. For the avoidance of doubt, references to ‘the Agreement’ mean this Call-Off Contract between the Supplier and the Authority. References to ‘the Authority’ mean ‘the Buyer’ (the Commissioners for Her Majesty’s Revenue and Customs).
2. The Agreement incorporates the Authority’s mandatory terms set out in this Additional Buyer Terms.
3. In case of any ambiguity or conflict, the Authority’s mandatory terms in this Additional Buyer Terms. will supersede any other terms in the Agreement.
4. **Definitions**

|  |  |
| --- | --- |
| **“Affiliate”** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| **“Authority Data”** | 1. the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:
	* + 1. supplied to the Supplier by or on behalf of the Authority; and/or
			2. which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or
2. any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;
 |
| **“Charges”**  | the charges for the Services as specified in Schedule 2 Call off Contract Charges |
| **“Connected Company”** | means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person; |
| **“Control”** | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly; |
| **“Controller”, “Processor”, “Data Subject”,** | take the meaning given in the GDPR;  |
| **“Data Protection Legislation”** | * 1. the GDPR, the LED and any applicable national implementing Laws as amended from time to time;
	2. the DPA 2018 to the extent that it relates to processing of personal data and privacy;
	3. all applicable Law about the processing of personal data and privacy;
 |
| **“GDPR”**  | the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **“Key Subcontractor”** | any Subcontractor:1. which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or
2. with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract;
 |
| **“Law”** | any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply; |
| **“Personal Data”** | has the meaning given in the GDPR;  |
| **“Purchase Order Number”**  | the Authority’s unique number relating to the supply of the Services;   |
| **“Services”**  | the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods; |
| **“Subcontract”** | any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof; |
| **“Subcontractor”** | any third party with whom:1. the Supplier enters into a Subcontract; or
2. a third party under (a) above enters into a Subcontract,

or the servants or agents of that third party; |
| **“Supplier Personnel”** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;  |
| **“Supporting Documentation”** | sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice;  |
| **“Tax”** | 1. all forms of tax whether direct or indirect;
2. national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;
3. all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and
4. any penalty, fine, surcharge, interest, charges or costs relating to any of the above,

in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction; |
| **“Tax Non-Compliance”** | where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC’s “Test for Tax Non-Compliance”, as set out in Annex 1, where:1. the “Economic Operator” means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and
2. any “Essential Subcontractor” means any Key Subcontractor;
 |
| **“VAT”** | value added tax as provided for in the Value Added Tax Act 1994. |

1. **Payment and Recovery of Sums Due**

The Supplier shall invoice the Authority as specified in Call off charges and payments of the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number: the Supplier does so at its own risk; andthe Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.* 1. Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority via the Authority’s electronic transaction system.
	2. If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority.  The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.
1. **Warranties**
	1. The Supplier represents and warrants that:
		1. in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;
		2. it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and
		3. no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier’s assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.
	2. If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.
	3. In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).
2. **Promoting Tax Compliance**
	1. All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.
	2. To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.
	3. The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.
	4. If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:
		1. notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and
		2. promptly provide to the Authority:
3. details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and
4. such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.
	1. The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.
	2. Upon the Authority’s request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.
	3. If the Supplier:
		1. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this may be a material breach of the Agreement;
		2. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or
		3. fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause). * 1. The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.
1. **Use of Off-shore Tax Structures**
	1. Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract (**“Prohibited Transactions”**). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties’ business.
	2. The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.
	3. In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.
	4. Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).
2. **Data Protection and off-shoring**
	1. The Processor shall, in relation to any Personal Data processed in connection with its obligations under the Agreement:
		1. not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
	2. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
	3. the Data Subject has enforceable rights and effective legal remedies;
	4. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
	5. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
	6. Failure by the Processor to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

**Annex 1****Excerpt from HMRC’s “Test for Tax Non-Compliance”***Condition one (An in-scope entity or person)*1. There is a person or entity which is either: (“X”)
2. The Economic Operator or Essential Subcontractor (EOS)
3. Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities’ financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts[[1]](#footnote-1)*;
4. Any director, shareholder or other person (P) which exercises control over EOS. ‘Control’ means P can secure, through holding of shares or powers under articles of association or other document that EOS’s affairs are conducted in accordance with P’s wishes.

 *Condition two (Arrangements involving evasion, abuse or tax avoidance)*1. X has been engaged in one or more of the following:
	1. Fraudulent evasion[[2]](#footnote-2);
	2. Conduct caught by the General Anti-Abuse Rule[[3]](#footnote-3);
	3. Conduct caught by the Halifax Abuse principle[[4]](#footnote-4);
	4. Entered into arrangements caught by a DOTAS or VADR scheme[[5]](#footnote-5);
	5. Conduct caught by a recognised ‘anti-avoidance rule’[[6]](#footnote-6) being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. ‘Targeted Anti-Avoidance Rules’ (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;
	6. Entered into an avoidance scheme identified by HMRC’s published Spotlights list[[7]](#footnote-7);
	7. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

*Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))*1. X’s activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:
	1. In respect of (a), either X:
		1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[[8]](#footnote-8); or,
		2. Has been charged with an offence of fraudulent evasion.
	2. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.
	3. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
	4. In respect of (f) this condition is satisfied without any further steps being taken.
	5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

 For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re‑enacted from time to time including any implementing or successor legislation.  |
| **Alternative clauses:** | Not used |
| **Buyer specific amendments to/refinements of the Call-Off Contract terms:** | Not used |
| **Public Services Network (PSN):** | Not used. |
| **Personal Data and Data Subjects:** | Confirm whether either Annex 1 or Annex 2 of Schedule 7 is being used: Annex 1  |

**1. Formation of contract**

1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
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.
3. This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
4. In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

**2. Background to the agreement**

1. The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.11.
2. The Buyer provided an Order Form for Services to the Supplier.

|  |  |  |
| --- | --- | --- |
| **Signed:** | Supplier | Buyer |
| **Name:** |  |  |
| **Title:** |  |  |
| **Signature:** |  |  |
| **Date:** |  |  |

## **Schedule 1 - Services**

TP Catalyst inclusive of access to royalties and commodities

* Named users for Portal: 10,000
* Concurrent licences for Portal: 999 per product
* Authorised usage for Portal: Unlimited

License Restrictions:

Unless specified otherwise,

1. Buyer may download, save, or print out limited excerpts of data contained in the licenced Information solely as required by it in pursuance of it permitted use of the licenced Information as set out as above. Buyer shall not download, copy, save or print out, on any one occasion or in a series of occasions, the data and/or information contained in the products set forth above so as to obtain a version of all or a substantial part of such data and/or information;
2. Buyer shall not and shall procure that none of its affiliates or their respective employees and consultants shall, use the Information to create a product which (a) competes with Supplier’s or any of its licensors or (b) provides the same or substantially similar functionally, content or features to such Information, as applicable;
3. The above license includes access for the specified number of users (“Users”) noted above at the permitted location. Each User is assigned a specific password to access and use the products and/or services described above (the “Information”). The Information and associated password(s) may only be used on behalf of the Buyer.

TP Catalyst

TP Catalyst combines company information with royalty rates, lending margins and our commodities modules so you can do transfer pricing analysis in an efficient, user-friendly workflow.

It simplifies transfer pricing analyses, including profit and transaction-based analyses. Developed in conjunction with TP specialists, TP Catalyst streamlines processes and reduces data manipulation.

Features

* Establish independent arm’s-length benchmarks for pricing intra-group transactions
* Conduct due-diligence review of external comparables
* Conduct BEPS risk-assessment analysis from a corporate-group perspective
* Monitor transfer pricing policies on an on-going basis
* Conduct BEPS risk-assessment analysis from a local-entity perspective

Benefits

* Extensive corporate ownership data
* Coverage of companies around the globe, with detailed financials
* 60,000 royalty rates
* 9,000 third-party loan tranches
* 4.5 million commodities prices
* original scanned documents
* intellectual property profiles
* financial stability indicators

**Coverage**

Data for all active entities registered at local registry offices globally.

- 270 million active entities.

Data for all inactive entities that were active companies registered at local registry offices globally.

- 85 million inactive entities.

Original documents filed at LRO or other Information Provider/source.

**Search Functionality**

An integrated tool that allows the user to combine various search criteria and select specified outputs.

A tool that allows you to create TP analyses and benchmarks

Test company

Review company

Benchmark company

Analysis tools to review groups/sets of companies

Ability to search through current and previous data. E.g. when searching for a company name the results will show hits on both current and previous company names.

Search results will display key identification details of each company.

- Results displayed can be customised using any data available.

- Each company can be selected to provide more details about that company"

**Data and Search Capability**

Ability to search on the following:

Companies

Commodities

Royalties

Loans

Ability to search on the following once analysis/es created:

Company name search

- Ability to search previous names

- Option for partial matching or whole word matching

- Option to match first word only

Identification number, e.g. VAT, CRN, Ticker symbol, ISIN number to find company name.

- Batch search ability up to 1m inputs.

Company status e.g. active, active (dormant), dissolved, in liquidation, insolvent etc.

Date company was liquidated/dissolved

Status

- Standardised legal form: Public, Private, Partnership, Sole trade/proprietorship, Public authority, Nonprofit, Branch, Foreign company, Other legal form

- National legal form: Select from each country specific legal forms e.g Germany general partnership - OHG

- Legal events: Registration, change in articles, management, ownership, auditor, bank, financials, agreement, licenses and certificates, reorganisation, default, termination, deregistration, judgement. Includes Date, description, source

Incorporation date - period.

Phone & URL, social media contact details

- Phone number or phone prefix

- Website address

- List of companies with a:

- Website or email

- Phone number

Location.

- World regions, country or region in country, NUTS classification, City, Postcode, Street address, US zip code radius, US Metropolitan Statistical Areas

Activities and Industry

Industry classifications: NACE Rev.2, US SIC, NAICS 2017, Code type

- Nomenclature of Economic Activities (NACE) rev 2

- US SIC

- North American Industry Classification System (NAICS) 2012

Entity type including: Bank, financial company, insurance company, corporate, private equity firm, venture capital, hedge fund, mutual and pension fund, foundation/research institute, public authority/state/government, marine vessels Specialisation Activity text search including free word search on actvity labels, trade description, desription and history, products and services, additional information Major sectors Public interest entities

Financials & ratios Key financials & employees: search functionality for up to 10 years for absolute numbers, growth and decline rates, including estimates. Global detailed financials: search functionality on balance sheet and p&l account Global standard format: search across internationally standardised financial accounts Global ratios TP specific rations: specific variables to search, taken from the global standard format TP Profit Level Indicators: specific variables to search, taken from the global standard format

Financial Strength Scores provided by multiple provides e.g CRIF, Zanders, modeFinance

Directors

Companies with director with specified name (free text and selectable) with following options:

- Current directors

- Previous directors

- Limit to shareholders

- Limit to individuals

- Exclude disqualified directors

- Position (company secretary, LLP member, other)

- Occupation

- Appointment date

- Resignation date

- Gender

- Nationality

- Address

- Age

- DOB Auditors, bankers and other advisors: name and country

Ownership

- Ultimate owners with: subsidiares by profile including type, size, country or region

-Shareholders with: subsidaires by profile including type, percentage between 0-100, size, country or region; subsidiaries by name; foreign subsidiaries; specific number of subsidiaries - Subsidiaries with: shareholders by profile including type, percentage between 0-100, size, country or region; shareholders by name, ultimate owners by profile including; foreign shareholders, shareholder also manager; specific number of shareholders, beneficial owners by profile including location; beneficial owners by name

- Branches and headquarters:

- Affiliates

- PEPs, sanctions and enforcements: LexisNexis WorldCompliance matches including by category - State-owned enterprises - Direct and Indirect Ownership searching within ownership explorer - Power and coalitions of shareholders, coalition analysis

Accounts type & availability

Account type e.g. full, group and exempt, etc.

Accounting Practice: IFRS, Local GAAP, Regulatory

Accounting Template: Banks, Corporates, Insurance      Accounts available: latest year of accounts, closing month of latest accounts, years with available accounts, number of years with accounts"

"Stock Data

Listing status, listed or unlisted

Stock exchanges, e.g. AIM Italia, London Stock Exchange, SEAQ, etc.

FTSE indexes, FTSE 100, FTSE 250, etc.

Current market capitalisation

Merger & Acquisition

Company role such as acquirer, vendor, etc.

Deal period, including event such as announced or completed.

Deal value

Deal multiple using EBITDA (Earnings before Interest, Tax, Depreciation and Amortisation), total assets etc.

Deal type, e.g. merger, demerger, etc.

**Individual Company Information**

Individual Company Information

Standard or full report templates and that can be customised to show the key and relevant data from the information held on the company. They include the following headings:

- Contact Details

- Legal & accounts info

- Size & main activity

- Industry research

- Financial data & ratios, can select point in time required

- Custom variables

- Credit data & CCJs

- Gazette data

- Stock data

- Directors & contacts

- Ownership

- Organisational Structure including visual group structure that is exportable - Beneficial owners and Power and Colations where available - Mortgage data

- Filing details

- Advisors & auditors

- Trading addresses

- News & deals

- Notes

- Peer report

 Intelligent linking in the reports, e.g. links to parent or subsidiary companies

 Access to original documents filed at companies house

 Ability to export various sections of the report.

**Analysis tools**

Pivot analysis

The following segments can be analysed as total, sub and customised populations:

- Region

- Industry classification

- Other key items such as legal for, incorporation date, credit score, auditors

- Financial data such as Turnover, Profit & Loss, Total assets and number of employees, key ratios, etc.

 The above items can also be shown as the measures and outputs for segment analysis

- Default template for industry/region & region/turnover

Peer analysis on selected population (2 to 2,500 companies)

Ownership Explorer

Geographical Heat Map

Statistical analysis covering items such as median, standard deviation, average, quartiles etc.

Concentration analysis with outputs in tabular and graphical forms such as pie charts or Lorenz curves.

Linear regression analysis e.g. turnover vs employees with tabular and regression chart.

**Other**

Ability to save search strategies, list formats within the tool.

Ability to save search exports and analysis locally.

Ability to export up to 500,000 lines of data

- Can split up exports into batches to export larger amounts of data.

- Various formats Microsoft Excel Workbook (.xlsx), Text File (.txt) with customized delimiters, etc.

Alert functionality.

- Send the user an email if specified criteria met.

E.g. changes in company name, liquidation, new accounts, change in auditors, etc.

Regular updates

Save favourite searches

Search history

Settings to set or change key features, e.g. default export settings, default ultimate owner definition.

Manage user defined fields, custom variables or own classifications.

Help options appropriate to each screen.

General help guide and manual

Training e.g. webinars, face to face training etc.

Telephone help from technical specialists

Contact function or feedback

Support for technical issues.

**Critical Success Factors**

**UK & Worldwide Data services**

Intuitive interface, that allows use with minimal training.

Powerful enough to create custom models, e.g. create a custom solvency model for specific customers

 ○ Ability to limit model by bulk input of Company Registration Number (CRN)

 ○ Ability to create & save our own custom variables from key financial data

 ○ Ability to save report and rerun them regularly.

 ○ Ability to run the report against new companies or new accounts.

Batch search on customer names past and present in order to find the CRN for matching purposes.

Export the latest SIC codes and the associated CRNs to excel to allow for sector analysis.

For an individual find all companies they hold share in and are directors off.

 ○ Be able to investigate the amount of shareholdings, class, date obtained and original documents.

In respect of the diverted profits tax, access to worldwide group structures

 ○ Accounts will be available for countries where companies file accounts from some countries.

Exporting data from in order to feed into our systems for further analysis. In particular the Large Businesses.

Export worldwide group structure.

**Transfer Pricing Tool**

The transfer pricing reports we create must be created using a tool that meets the industry standards.

 ○ The tool needs to have access to a comprehensive and large source of data.

 ○ The ability to create reports with sufficient detail.

 ○ The ability to perform all the currently used Transfer Pricing methodologies and regularly update them.

Ability to export data from Transfer Pricing Tool and import into worldwide data service to obtain further information.

Ability to re-perform the comparative analysis exercises produced by Groups in their Transfer Pricing reports.

**Technical and other**

Minimum of 10k user accounts.

Fast searches and analysis

 ○ 90% of searches to return within 10 seconds.

 ○ 90% of exports to complete within 3 minutes.

 ○ 90% of analysis to complete within 3 minutes"

has the ability to create Client specific sectors and run pre-defined and ad-hoc reports;

can cover a broad range of UK industries (Overseas if available), making use of government industry classification (SIC codes – at 5 digit ‘class’ level);

has a query tool enabling the Client to search across the entire UK economy (Overseas if available) at the granular industry level; to cover statistics, cost structure, levels, trends, risks, supply chain, external drivers, regional concentration; and

covers the subject – commodity; financial market; content types; corporate or industry type; economic; trends and analysis; international; political; sport and recreation.

**Reporting Tool Functionality**

Market characteristics

Current and historical performance for each industry

Future forecasts on revenue, imports, exports, employment and other key statistics

Summary level industry/sector analysis

Trends

Industry Research Reports – UK (and overseas if available)

Visual representations of key data (graphs, charts etc.

UK Business Environment and its impact on each industry

Market segmentation

Key supplier profiles

Public sector analysis

Provides information on related industries and external business environment.

**Risk Analysis**

Risk Rating Reports.

**Industry Sectors Required**

Product Intelligence

Summary level industry/sector analysis

Trends

Market Research Reports – UK (and overseas if available)

Visual representations of key data (graphs, charts etc)

UK Consumer Environment and its impact on industries

Provides information on businesses within markets, related industries and operating environment.

**Identify Future Risk**

Functionality to provide strategic assessments of emerging trends to identify future risk areas to help understand:

Threats and opportunities presented by consumers (End or B2B) to industry over coming period Partially relevant. May be available within industry research, dependent on the sector.

Industry structure, including size/scale and market share data Partially relevant. May be available within industry research, dependent on the sector.

**Search tool functionality**

Allow users to combine various search criteria and select specified outputs

Ability to run bespoke reports against UK economy.

Reports and data to be available to user for extraction by following options (Indicative) – email; print; save search or alert; downloadable by way of multiple file types and interfaces [e.g. RTF/PDF/XML/DOC/HTML/Plain text/attachments/API/JSON

Based on up-to-date data from official, recognised, sources

Regularly updated – maximum interval for renewal of reporting is annual

Published in consistent report formats, to enable comparison between reports.

Saved searches held on Supplier infrastructure (portal) must be secure

**Service Level Agreement**

1. Summary of the Service Level Agreement (SLA) for TP CATALYST

A distinction is made between:

- The technical support, which is provided by Supplier in case TP CATALYST (or specified product) or one of its components is not working properly;

- The functional support, which is provided in case a user of TP CATALYST has questions relating to the use of TP CATALYST (or one of its components) or the data available in a specific update of TP CATALYST

Supplier will provide:

- Technical support to Buyer should any issues arise over access to TP CATALYST directly. Buyer will also be responsible to inform Supplier in due time of any technical problem that might arise.

- The functional support (e.g questions relating to the use of the software as well as regarding the data) directly to users of TP CATALYST.

2. Service Level Agreement (SLA) for TP CATALYST

2.1 Support:

(a) Supplier shall make all reasonable commercial efforts to provide support services: Telephone and e-mail support is provided in London continuously from 8:30AM to 6:30PM GMT Monday to Friday (collectively, “Telephone Support Hours”). After 6.30pm GMT telephone support will be available via New York and then Singapore. For Severity 1 level errors Supplier shall make all reasonable commercial efforts to provide telephone support. Supplier shall respond to service requests and correct Errors in accordance with the severity levels reasonably agreed between Subscriber and Supplier as follows:

SEVERITY LEVEL TELEPHONE RESPONSE TIME (see (b) below)

Severity 1 thirty (30) minutes

Severity 2 one (1) hour

Severity 3 three (3) hours

A Severity 1 Error causes the Supplier Service to cease: (a) operating, or (b) operating in any material respect. A Severity 1 Error shall include any Error in the software component of the Supplier Service that poses imminent harm to Subscriber’s computer systems.

A Severity 2 Error causes a minor function of the Supplier Service to be impaired but will not significantly impair users from utilising the Supplier Service.

A Severity 3 Error causes a minor function of the Supplier Service to be impaired; however there is no adverse affect on Subscriber’s business.

(b) Supplier will respond to telephone service requests pursuant to the Response Times during Telephone Support Hours. Outside of Telephone Support Hours, Severity 3 Errors shall be e-mailed to help.london@bvdinfo.com, who will respond within three (3) hours of the next start of Telephone Support Hours.

Telephone Support London / New York / Singapore

0207 549 5050 / 1 (212) 797 3550 /+65 6325 1230

Outside Telephone Support Hours for Severity 1 level errors

00 32 478 888034

Supplier will use all reasonable commercial efforts to correct Severity 1 Errors within two (2) hours and Severity 2 Errors within eight (8) hours, and Supplier will assign a senior engineer to work on such Errors until the problem is corrected, however Supplier cannot guarantee the correction time. Severity 3 Errors will be discussed and Supplier will make reasonable attempts made to diagnose them within the response time. The time for correction of Severity 3 Errors will be discussed between the parties and mutually agreed to on a case-by-case basis.

Supplier will use all reasonable commercial efforts to have Content Providers correct errors caused by them, however correction times for all Content caused errors, except for Supplier caused errors, are excluded.

2.2 Service Availability:

The Services will be operational and fully functional in all material respects (i.e. capable of displaying information and conducting transactions as contemplated in the ordinary course of business) 99% of the time during any 30 day period. The parties shall mutually agree upon a regularly scheduled maintenance downtime period, which shall not exceed two hours in length per day and shall occur during “off-peak hours”. The scheduled maintenance period will be between Friday 11pm GMT and Monday 8am GMT time. On occasions Supplier may need to do maintenance which exceeds 30 minutes. In such cases advance warning of not less than 3 business working days will be given as to the time and length of downtime.

2.3 Security:

Supplier will use its best efforts to prevent unauthorized access to restricted areas of its servers and any databases or other sensitive material generated from or used in conjunction with the Services. In addition, Supplier will immediately notify Buyer of and take action to remedy any known security breaches of the system. If it is a technical issue at Supplier, Supplier will be responsible for the costs. If it is due to Buyer not managing their user IDs or providing access to the Supplier Services by users outside contracted area then Buyer will be responsible for any costs.

2.4 Browser Compatibility:

• Windows XP, Vista or 7

• Minimum screen resolution of 1024×768

• Access to the Internet using either Internet Explorer 7, Firefox 2 or higher, or Google Chrome

2.5 Redundancy:

The Services will operate with redundancy of the data store, application servers, and web servers. Supplier will use all reasonable efforts to monitor the status and availability of all components associated with the delivery of the Services.

3. Responsibilities

3.1 Responsibilities of Supplier

Supplier is responsible for the support of TP CATALYST and its interfaces and will:

• solve incidents and problems of the application if those can be reproduced within the time set;

• communicate about the progress/status of incidents and problems will be reported to Buyer;

• communicate to Buyer (rissystems.datamgt@hmrc.gov.uk) providing a minimum of 25 days’ notice if there are software changes, including screen changes, due and when they will be implemented;

• directly support the users with any questions relating to the functionality of the application or the data available on TP CATALYST.

• act as a single point of contact for Supplier for technical and functional issues. For data issues and updating of content supplier can be contacted directly.

3.2 Responsibilities of Buyer

Buyer is responsible for:

• informing Supplier about any incidents / problems and required changes through the agreed communication channel;

• using the application in an appropriate way

**Training**

HMRC is responsible for the creation and removal of users. All end users must first access the HMRC External Systems Intranet Page which identifies which HMRC team to contact, for example the RIS data management team (rissystems.datamgt@hmrc.gov.uk) to request a login, the request will then be forwarded to the relevant BvD administration team internally.

Training requests must also be sent to the RIS data management team. This is then passed to your Account Director who coordinates with the CS team.

The CS team have been introduced to some regional CPD representatives across the UK and will require introductions to all. This function enables BvD to provide training to a wider audience and to deliver this in an efficient manner.

Supplier will provide onsite training in the main Buyer hubs to encourage use of the tax risk solutions and to support the use of the new interfaces.

Local offices must request training using the process above if this is more suitable for end users.

Online training will be delivered via Zoom or HMRC equivalent in instances where HMRC employees are unable to receive training in person.

Walk-me guides are available within Fame and Orbis to help new and existing users navigate around the new interfaces. Within these guides are also video tutorials that have been specially designed for tax authorities. Support from the BvD helpdesk (020 7549 5050) is available 0800-1800 5 days per week, this will be 24 hours 6 days a week from May 2020.

A minimum of 2 onsite training sessions will be delivered per quarter. Online training will be delivered on request.

|  |
| --- |
| **Security Plan** |
|  |
|  **1 Policy & Standards** |
| **1a** Please confirm that you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.* **Yes**
 |
| **1b** Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from [Security Policy Framework](https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework) and any Security Requirements recorded in the schedules and/or Order Form.* **Moody’s has an Information Security Program governed by Information Security Policy. Moody’s confirms to the requirements set out by it’s Information Security Policy.**
 |
| **1c** If you believe that the [Public Sector Network (PSN)](https://www.gov.uk/government/groups/public-services-network) Code of Connection, available from www.gov.uk, will apply to your organisation and any sub-contractors, please provide details of how you will conform to this.* **No**
 |
| **1d** Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the General Data Protection Regulation see [GDPR](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) and in accordance with Clause 23 (*Protection of Personal Data*) of the Contract.* **Yes**
 |
| **1e** Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found [here](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/)* **Yes**
 |
| **1f** Please provide details of any security accreditation that your organisation currently possesses, such as but non exclusive to, ISO 27001 and PCI DSS and describe the process used to achieve the accreditation.* **Moody’s currently do not possess security accreditations**
 |
| **1g** If you intend to involve sub-contractors at any stage during the Contract please list them and provide details of how you will ensure their compliance with all aspects of this Security Plan.* **Moody’s Vendor Risk Management group is responsible for managing third party compliance**
 |
| **1h** As appended to this Schedule 2.4, Appendix G, Security Aspects Record, defines the Government Security Classifications (see [Government Security Classifications](https://www.gov.uk/government/publications/government-security-classifications)) carried by the HMRC data. If you are successful in the tender process, you will require a Security Manager (or appointed person), to take responsibility for the security of the data. Please provide the name of your Security Manager who will act as a first point of contact and conduct ongoing management of security risks and incidents (including identification, managing, and reporting in line with agreed procedures for actual or suspected security breaches).* **Amelia Webster is the primary client contact**
 |
| **2 Physical Security** (For requirements please see Appendix A – Physical Security) |
| **2a** For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter.Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site.Please also provide details of the maintenance schedule of your security controls.* **Physical access controls have been implemented for all data centres where Business Data is stored, including 24x7 onsite staff, biometric scanning, and security camera monitoring on entry doors. Moody’s Analytics hosted products are hosted in 3rd party co-location data centers. The 3rd party data center services vendors include Interoute and Interxion. Both Interoute and Interxion are ISO 27001 certified.**
 |
| **2b** Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas within the premises holding HMRC assets.Detail measures such as building construction type, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls.* **BvD office in Brussels and Moody’s Analytics office in New York and London are main offices. Physical security controls include 24x7 onsite staff, biometric scanning, and security camera monitoring on entry doors.**
 |
| **3 IT Security** (For requirements please see Appendix B – IT Security)  |
| **3a** Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed or provide details of any cyber essentials accreditation that you are planning in the future.* **NA**
 |
| **3b** Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention), and how regularly you update them.* **Moody’s has formal policies, standards and procedures under Information Security Program. The documentation includes but is not limited to Patch Management Standard, Anti-Virus Procedure, Network Security Standard. Moody’s has implemented Endpoint Security tools on all systems and has SafeSend to ensure sensitive data is not sent outside Moody’s network**
 |
| **3c** Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users.* **Moody’s has a formal User and Access Management Standard**
* **Moody’s maintains policies and procedures that define the requirements for access to information, including approvals, onboarding and off-boarding requirements, password requirements, segregation of duties, periodic user access recertification, and the logging/monitoring requirements and mechanisms. ServiceNow ticketing system is used to track access requests and approvals and SailPoint is used to manage identity and access.**
* **Privileged Access Management (PAM) solutions are used to log and monitor use of privileged access. Privileged accounts are reviewed and recertified periodically. Remote access to Moody’s corporate network is via VPN and requires two factor authentication (2FA). System access for terminated personnel is removed within 24 hours**
 |
| **3d** Please provide details of how your security and access control policy complies with the Security Policy Framework (including where necessary, use and control of backup systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets). * **Client data is segregated logically on Moody’s systems. Access to sensitive data is granted based on the least privilege principal. Privileged access is reviewed and recertified quarterly**
 |
| **3e** Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing).* **Moody’s has a formal Secure SDLC standard for in house development. Any procured software or new patches are tested in non-prod environment and go through a formal change management process. Additionally, Moody’s perform annual penetration testing conducted by a third party**
 |
| **3f** Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data.* **Write access to removable media is blocked on all Moody’s systems to ensure that client data is not copied on external devices. Backup devices stored at third party location are encrypted at rest.**
 |
| **3g** Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with HMG Security Policy Framework requirements for information management. * **IT Asset Disposal processes are followed to prevent data loss through full destruction of Moody’s data stored on Moody’s hardware. The disposal process consists of:**
	+ **Coordination of the disposal with the Disposal Vendor. This may be documented through a signed Vendor Statement of Work (SOW)**
	+ **Certified data erasure, equipment shredding or degaussing by the Disposal Vendor**
	+ **Witnessing of the shredding by a Moody’s employee**
	+ **Provision of Certificate of Indemnification (COI)**
 |
| **4 Personnel Security** (For requirements please see Appendix C – Personnel Security) |
| **4a** What security vetting has been carried out for staff who will have access to or come in to contact with HMRC data or assets.* **Moody’s only allow persons to have access to Business Data who have undertaken background security checks of a type and scope that are normal and customary for the financial services industry and comply with applicable law. Such background checks include address and employment history verification, the right to work in the relevant jurisdiction, screening against databases of individuals subject to economic sanctions and, if permitted by applicable law, criminal records checks. Moody’s exclude any of its personnel from accessing the Business Data (i) whose background check reveals they have been convicted of any criminal offense involving dishonesty or breach of trust, including money laundering or any criminal offense concerning the illegal manufacture, sale or distribution of or trafficking in controlled substances, (ii) who appear on any sanctions database or (iii) who are not authorized to work in the relevant jurisdiction.**
 |
| **4b** Please provide details of how you will ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract.* **All Moody’s are required to agree to Moody’s Code of conduct and get trained on Moody’s IT Use Policy which includes non-disclosure of client data**
 |
| **4c** All contractor’s personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC’s Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested.* **No contractors involved that handle HMRC data**
 |
| **4d** Please provide details of the ongoing training you provide to staff in respect of data security, including risk awareness and the identification and reporting of security incidents. Please also provide details of your documented information security procedures and processes that are available to all staff who will have access to or come into contact with HMRC data.* **Moody’s employees receive training on an annual basis, as well as upon hire, of the IT Use Policy. The IT Use Policy lays out the user-facing security controls including information classification and handling, acceptable use, usages standards for the main technologies, and other controls; as well as exceptions to the policy. The training course is updated yearly, and is mandatory for all employees and employees are required to agree to comply with the IT Use Policy.**
* **Moody’s has implemented an Anti-Phishing program using PhishMe and periodically sends out phishing test emails to employees to determine susceptibility rates and to target users for training who click on the phishing links.**
* **Developers, DevOps and related personnel also undergo Secure Software Development Lifecycle (SDLC) training, including training in Veracode Secure Application Secure Testing (SAST) tools.**
 |
| **4e** Please provide details of your procedures for on and off boarding staff* **On boarding staff includes interview process, background checks, access provisioning**
* **Off boarding includes exit interview, access decommissioning on the last day**
 |
| **5 Process Security** (For requirements please see Appendix D – Process Security) |
| **5a** Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed.* **All client data is logically segregated on Moody’s systems**
 |
| **5b** Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration.* **Client data will not be transferred to third parties**
 |
| **5c** Please confirm that you understand that HMRC data must not be processed or stored outside the United Kingdom without the express permission of HMRC. If you are considering storing data outside of the UK, please provide details on how and where the data will be stored and also provide details of how you comply with Cabinet Office policy for offshoring see [Offshoring](https://ogsirooffshoring.zendesk.com/hc/en-us/article_attachments/202389402/Offshoring_Information_Assets_Classified_at_OFFICIAL_v1.1.pdf)* **Client data resides within agreed upon geographical locations during contracting**
 |
| **5d** In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data, and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent.* **Moody’s has employed strong access controls such as segregation of duties, privileged access reviews, least privileged principle and access recertification**
 |
| **5e** What arrangements are in place for secure disposal of HMRC assets that may be in your possession once no longer required?* **Data disposal is conducted per client specifications**
 |
| **5f** How and when will you advise HMRC of security incidents that impact HMRC assets that may be in your possession?* **When an incident is deemed to affect the client data/systems, the client will be notified immediately via customer portal and /or customer representative**
 |
| **5g** Please describe your disciplinary procedures in the event of a security breach involving HMRC data.* **Moody’s has a formal Incident Response Plan which outlines process steps, roles and responsibilities, incident containment and forensic procedures (id required)**
 |
| **5h** Do you have a List X accreditation? If ‘yes’, please answer the following:* What is the name of your Security Controller?
* What/Where does the List X accreditation cover?
* For what purpose?
* Please provide evidence the Department who sponsored the List X accreditation has agreed to share the environment.
* **NA**
 |
| **6 Business Continuity** |
| **6a** Please provide an overview of your organisation’s Business Continuity and disaster recovery plans in terms of the HMRC data under the Contract, or attach a copy of your Business Continuity Plan. Please specify if you operate Business Continuity or disaster recovery from outside the UK.Also, please provide details on when and how frequently these plans are tested and advise when they were last tested and confirm results of testing exercises are available for review if requested. Please provide details on how you will meet recovery times if these have been specified in the schedules and/or Order Form.* **Moody’s has a formal BCP policy and BCP plan. BCP is tested annually.**
 |
| **7 Cryptography** |
| **7a** Please provide details of processes and procedures in place for handling Government cryptographic material.* **Moody’s does not handle Government cryptographic material**
 |

## **Schedule 2 - Call-Off Contract charges**

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

The total value of this Call-off Contract shall not exceed £400,000 excluding VAT as per the breakdown below:

* Year 1, TP Catalyst: £200,000
* Year 2, TP Catalyst: £200,000

## **Part B - Terms and conditions**

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

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

### 2. Incorporation of terms

1. The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
	* 4.1 (Warranties and representations)
	* 4.2 to 4.7 (Liability)
	* 4.11 to 4.12 (IR35)
	* 5.4 to 5.5 (Force majeure)
	* 5.8 (Continuing rights)
	* 5.9 to 5.11 (Change of control)
	* 5.12 (Fraud)
	* 5.13 (Notice of fraud)
	* 7.1 to 7.2 (Transparency)
	* 8.3 (Order of precedence)
	* 8.4 (Relationship)
	* 8.7 to 8.9 (Entire agreement)
	* 8.10 (Law and jurisdiction)
	* 8.11 to 8.12 (Legislative change)
	* 8.13 to 8.17 (Bribery and corruption)
	* 8.18 to 8.27 (Freedom of Information Act)
	* 8.28 to 8.29 (Promoting tax compliance)
	* 8.30 to 8.31 (Official Secrets Act)
	* 8.32 to 8.35 (Transfer and subcontracting)
	* 8.38 to 8.41 (Complaints handling and resolution)
	* 8.42 to 8.48 (Conflicts of interest and ethical walls)
	* 8.49 to 8.51 (Publicity and branding)
	* 8.52 to 8.54 (Equality and diversity)
	* 8.57 to 8.58 (data protection)
	* 8.62 to 8.63 (Severability)
	* 8.64 to 8.77 (Managing disputes and Mediation)
	* 8.78 to 8.86 (Confidentiality)
	* 8.87 to 8.88 (Waiver and cumulative remedies)
	* 8.89 to 8.99 (Corporate Social Responsibility)
	* paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
	* any audit provisions from the Framework Agreement set out by the Buyer in the Order Form
2. The Framework Agreement provisions in clause 2.1 will be modified as follows:
	* a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
	* a reference to ‘CCS’ will be a reference to ‘the Buyer’
	* a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract
3. The Parties acknowledge that they are required to complete the applicable Annexes contained in schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at schedule 7 of this Call-Off Contract.
4. The Framework Agreement incorporated clauses will be referred to as ‘incorporated Framework clause XX’, where ‘XX’ is the Framework Agreement clause number.
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

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.
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

1. The Supplier Staff must:
	* be appropriately experienced, qualified and trained to supply the Services
	* apply all due skill, care and diligence in faithfully performing those duties
	* obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
	* respond to any enquiries about the Services as soon as reasonably possible
	* complete any necessary Supplier Staff vetting as specified by the Buyer
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.
3. The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
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.
5. The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
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 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
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.
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

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

### 6. Business continuity and disaster recovery

1. The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.
2. The Supplier’s business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
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

1. The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.
2. The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
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.
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.
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.
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. All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.
8. The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
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.
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.
11. If there’s an invoice dispute, the Buyer must pay the undisputed 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.
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

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

### 9. Insurance

1. The Supplier will maintain the insurances required by the Buyer including those in this clause.
2. The Supplier will ensure that:
	* 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
	* the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
	* 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
	* 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
3. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
4. If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
	* a broker's verification of insurance
	* receipts for the insurance premium
	* evidence of payment of the latest premiums due
5. Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
	* + take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
		+ promptly notify the insurers in writing of any relevant material fact under any insurances
		+ hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
6. The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
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.
8. The Supplier will be liable for the payment of any:
	* premiums, which it will pay promptly
	* excess or deductibles and will not be entitled to recover this from the Buyer

### 10. Confidentiality

1. Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.78 to 8.86. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

### 11. Intellectual Property Rights

1. Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.
2. The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer’s ordinary business activities.
3. The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer’s right to publish the IPR as open source.
4. The Supplier must promptly inform the Buyer if it can’t comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can’t obtain the grant of a licence acceptable to the Buyer.
5. The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party’s IPRs because of the:
	* rights granted to the Buyer under this Call-Off Contract
	* Supplier’s performance of the Services
	* use by the Buyer of the Services
6. If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
	* modify the relevant part of the Services without reducing its functionality or performance
	* 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
	* buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
7. Clause 11.5 will not apply if the IPR Claim is from:
	* the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract
	* other material provided by the Buyer necessary for the Services
8. If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

### 12. Protection of information

1. The Supplier must:
	* comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data
	* 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
	* take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes
2. The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
	* providing the Buyer with full details of the complaint or request
	* complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions
	* providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
	* providing the Buyer with any information requested by the Data Subject
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

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

1. The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
2. If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
3. 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 policy and all Buyer requirements in the Order Form.
4. The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
5. The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
	* the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>
	* guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
	* the National Cyber Security Centre’s (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
	* government best practicei[n](https://www.cesg.gov.uk/risk-management-collection) [t](https://www.cesg.gov.uk/risk-management-collection)he design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
	* the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
6. The Buyer will specify any security requirements for this project in the Order Form.
7. 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.
8. 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.
9. 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

1. The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
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 available at](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary) <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
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.
4. If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
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[.](https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary)

### 15. Open source

1. All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
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

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.
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.
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.
4. Responsibility for costs will be at the:
	* 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
	* 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
5. The Supplier will immediately notify CCS of any breach of security of CCS’s Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
6. Any system development by the Supplier should also comply with the government’s ‘10 Steps to Cyber Security’ guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
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

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:
	* an executed Guarantee in the form at Schedule 5
	* 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

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.
2. The Parties agree that the:
	* Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
	* Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier’s avoidable costs or Losses
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.
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:
	* a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
	* any fraud
5. A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
	* 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
	* an Insolvency Event of the other Party happens
	* the other Party ceases or threatens to cease to carry on the whole or any material part of its business
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.
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

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.
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.
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.
4. Ending or expiry of this Call-Off Contract will not affect:
	* any rights, remedies or obligations accrued before its Ending or expiration
	* the right of either Party to recover any amount outstanding at the time of Ending or expiry
	* the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.87 to 8.88 (Waiver and cumulative remedies)
		+ 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
5. At the end of the Call-Off Contract Term, the Supplier must promptly:
	* return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
	* return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
	* 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
	* 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
	* work with the Buyer on any ongoing work
	* return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
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.
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

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** | **Deemed time of delivery** | **Proof of service** |
| Email | 9am on the first Working Day after sending | Sent by pdf to the correct email address without getting an error message |

1. 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

1. The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
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.
3. If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
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.
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.
6. The Supplier acknowledges that the Buyer’s right to extend the Term beyond 24 months is subject to the Buyer’s own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier’s additional exit plan ensures that:
	* the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
	* there will be no adverse impact on service continuity
	* there is no vendor lock-in to the Supplier’s Service at exit
	* it enables the Buyer to meet its obligations under the Technology Code Of Practice
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.
8. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
	* 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
	* 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
	* the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
	* the testing and assurance strategy for exported Buyer Data
	* if relevant, TUPE-related activity to comply with the TUPE regulations
	* 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

1. At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
	* data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control
	* other information reasonably requested by the Buyer
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.
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

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

### 24. Liability

1. Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:
	* Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
	* Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
	* Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

### 25. Premises

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.
2. The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.
3. The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.
4. This clause does not create a tenancy or exclusive right of occupation.
5. While on the Buyer’s premises, the Supplier will:
	* comply with any security requirements at the premises and not do anything to weaken the security of the premises
	* comply with Buyer requirements for the conduct of personnel
	* comply with any health and safety measures implemented by the Buyer
	* immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
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

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

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

1. The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
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)

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.
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:
	* the activities they perform
	* age
	* start date
	* place of work
	* notice period
	* redundancy payment entitlement
	* salary, benefits and pension entitlements
	* employment status
	* identity of employer
	* working arrangements
	* outstanding liabilities
	* sickness absence
	* copies of all relevant employment contracts and related documents
	* all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
3. The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
4. In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
5. The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
6. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
	* its failure to comply with the provisions of this clause
	* 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
7. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
8. For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

### 30. Additional G-Cloud services

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.
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

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.
2. In addition to any obligations under the Collaboration Agreement, the Supplier must:
	* work proactively and in good faith with each of the Buyer’s contractors
	* 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

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.
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.
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, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Call-Off Contract document at schedule 7

## **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 Section 2 (Services Offered) 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 Digital Marketplace). |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any). |
| **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 TaxAct 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |
| **Controller** | Takes the meaning given in the 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 Framework Agreement 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** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection Legislation (DPL)** | Data Protection Legislation means: 1. (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time
2. (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy;
3. (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
 |
| **Data Subject** | Takes the meaning given in the 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. |
| **Deliverable(s)** | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract. |
| **Digital Marketplace** | The government marketplace where Services are available for Buyers to buy. (<https://www.digitalmarketplace.service.gov.uk>/) |
| **DPA 2018** | Data Protection Act 2018. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) which implements the Acquired Rights Directive. |
| **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 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:<http://tools.hmrc.gov.uk/esi> |
| **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 RM1557.11 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 Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| **GDPR** | 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 https://www.gov.uk/government/publications/government-procurement-card--2. |
| **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.
 |
| **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 client 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 client 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 CCS’s possession before the Start Date. |
| **Law** | Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body. |
| **LED** | Law Enforcement Directive (EU) 2016/680. |
| **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 section 6 (What you report to CCS). |
| **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 GDPR. |
| **Personal Data Breach**  | Takes the meaning given in the GDPR. |
| **Processing** | Takes the meaning given in the GDPR |
| **Processor** | Takes the meaning given in the GDPR. |
| **Prohibited Act** | To directly or indirectly offer, promise or give any person workingfor or engaged by a Buyer or CCS a financial or other advantageto:* 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: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of 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 G-Cloud 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 Section 2 (Services Offered) of the Framework Agreement. |
| **Service Description** | The description of the Supplier service offering as published on the Digital Marketplace. |
| **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-controls-check-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 G-Cloud 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 - GDPR Information**

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

## **Annex 1 - Processing Personal Data**

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

* + - 1. The contact details of the Buyer’s Data Protection Officer are:
			2. The contact details of the Supplier’s Data Protection Officer are: **Not applicable**
			3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
			4. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Parties are Independent Controllers of Personal Data**The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* 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,
* Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer engaged in the performance of the Buyer’s duties under the Contract for which the Supplier is the Controller.
* Any Personal Data contained in the G-Cloud Services that may be transferred to Buyer and/or that Buyer may access, including by downloading, saving or printing, for which the Buyer is the Controller.

  |
| Duration of the Processing | Until conclusion of the purpose for processing. |
| Nature and purposes of the Processing | In relation to the business contact details as specified above, collection and use for the purposes of, including but not limited to, account management, invoicing, collection of licence fees, and/or managing access to content and service.In relation to the Personal Data contained in the G-Cloud Services, for the Buyer’s internal business purposes. |
| Type of Personal Data | Names and business contact details such as job titles, emails and/or telephone numbers |
| Categories of Data Subject | Employees, agents, consultants and contractors, UK and international company directors |
| Plan for return and destruction of the data once the Processing is completeUNLESS requirement under Union or Member State law to preserve that type of data | Deletion or destruction upon conclusion of the purpose for processing. |

##

1. <https://www.iasplus.com/en/standards/ifrs/ifrs10> [↑](#footnote-ref-1)
2. ‘Fraudulent evasion’ means any ‘UK tax evasion offence’ or ‘UK tax evasion facilitation offence’ as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act. [↑](#footnote-ref-2)
3. “General Anti-Abuse Rule” means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any

future legislation introduced into Parliament to counteract tax advantages arising from abusive

arrangements to avoid national insurance contributions [↑](#footnote-ref-3)
4. “Halifax Abuse Principle” means the principle explained in the CJEU Case C-255/02 Halifax and others [↑](#footnote-ref-4)
5. A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992. [↑](#footnote-ref-5)
6. The full definition of ‘Anti-avoidance rule’ can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly. [↑](#footnote-ref-6)
7. Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: <https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight> [↑](#footnote-ref-7)
8. The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed. [↑](#footnote-ref-8)