Crown Commercial Service

G-Cloud 13 Call-Off Contract

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

G-Cloud 13 Call-Off Contract

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	9875 3374 9482 791
Call-Off Contract reference	TIS0632
Call-Off Contract title	Partner to Support, Change & Maintain the Insolvency Service Instance of Unit4 ERP
Call-Off Contract description	The services of a partner to support, change and maintain the Insolvency Service instance of Unit4 Enterprise Resource Planning (ERP) Software Solution (Version ERP7).
Start date	29th January 2024
Expiry date	26 July 2026 Unless extended in accordance with the extension period
Call-Off Contract value	£262,250 With the optional extension option increasing this to £361,150 Subject to indexation in accordance with Schedule 2 The contract has provision for additional activities to be procured up to the value of £195,575 in accordance with the rate card provided at Schedule 2. These will be agreed via the change control process Maximum Contract Value: £556,725 (subject to indexation)
Charging method	Purchase Order – Invoice - BACS
Purchase order number	To be confirmed: 60000xxxx (Provided once contract is signed)

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

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

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

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

From the Buyer	The Insolvency Service **REDACTED**
To the Supplier	Vision ERP Limited **REDACTED**
Together the 'Parties'	

Principal contact details

For the Buyer:
Title: Commercial Business Partner
Name: REDACTED
Email: REDACTED
Phone: REDACTED

For the Supplier:
Title: Director
Name: REDACTED
Email: REDACTED
Phone: REDACTED

Call-Off Contract term

Start date	This Call-Off Contract Starts on 29th January 2024 and is valid for 30 months until 26th July 2026
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **one month's** written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

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

G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 3: Cloud support
G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below: • Unit4 ERP (Business World/Agresso/U4BW) Consultancy

Additional Services	• Cloud Support
	• Implementation
	• Project Management
	• Consultancy
	• Integrations
	• Support
	  ○ Report Writing
	  ○ Data Migration

Location	The Services will mostly be delivered remotely by the Supplier
Quality Standards	The Requirement's detailed in document in Annex 1. "REQUIREMENTS" set out the Authority's minimum expectations for an operational service.
Technical Standards:	Not used
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are **contained with Schedule 1 – Services**
Onboarding	The onboarding plan for this Call-Off Contract is **contained in Schedule 1 – Services**
Offboarding	The offboarding plan for this Call-Off Contract is **to be agreed and confirmed in line with Clause 21 – Exit Plan**

Collaboration agreement	Not used
Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed **125%.** The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed **125%** the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed the greater of **125%** the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).

Insurance	The Supplier 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
Buyer's responsibilities	The Buyer is responsible for. • The Authority will be responsible for: • Supporting the onboarding of service provider • Providing necessary documentation and information in relation to our ERP instance to deliver the contract. • Providing the supplier with known change and development requests and agree the process for delivery between both parties (e.g., issue of service development request forms) • Where development is required, providing the service provider with appropriate SME (Subject Matter Experts) support for tasks such as: user acceptance testing and reviewing development requirements. • Informing the supplier of any changes in our security requirements • Provide the supplier with information about steps to take to onboard and integrate into our SIAM ecosystem.

Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes: ERP SaaS Software and associated services **Reason:** As this is the software/system that the supplier will support and provide consultancy services for.

Supplier's information

Subcontractors or partners	Not used

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: See Schedule 2: Call-Off Contract charges
Invoice details	The Supplier will issue electronic invoices for the fixed costs monthly/annually in arrears in advance The Buyer will pay the Supplier within 30 days of receipt of a valid invoice Before payment can be considered each invoice must include details of work completed/to be completed. Each invoice shall also contain the Contract Title and Contract Reference number: TIS0632 and a valid Purchase Order Number which will be provided by the Buyer. The Insolvency Service recognises the importance of prompt, fair and effective payment in all businesses. Being

	paid promptly for work done ensures businesses have a healthy cash flow. In accordance with the Regulations, the Insolvency Service includes 30 calendar day payment terms in all new public sector contracts and will work with contracted suppliers to ensure that this payment term is passed down the supply chain. To support this commitment, the Insolvency Service operate a No PO (Purchase Order) No PAY (Payment) policy. All Invoices must comply with the No PO No Pay Policy to be considered valid and be paid. A valid Supplier Invoice shall include the following: • Valid Insolvency Service Purchase Order Number; • Insolvency Service Contract Reference Number (if applicable); • Invoice must accurately map to the line items within the Purchase Order, i.e. Line Descriptions, Number of Units and Unit Price The Insolvency Service may make reasonable changes to its invoicing requirements during the Term of the contract by providing 30 calendar days written notice to the Supplier. All payments are subject to approval of the Buyer.
Who and where to send invoices to	Invoices will be sent to payments@insolvency.gov.uk
Invoice information required	All invoices must include: 1. Valid Insolvency Service Purchase Order Number; 2. Insolvency Service Contract Reference Number TIS0632; 3. Invoice must accurately map to the line items within the Purchase Order, i.e., Naming, Number of Units and Unit Price.
Invoice frequency	Invoice will be sent to the Buyer monthly in arrears.

Call-Off Contract value	£262,250 With the optional extension option increasing this to £361,150 Subject to indexation in accordance with Schedule 2 The contract has provision for additional activities to be procured up to the value of £195,575 in accordance with the rate card provided at Schedule 2. These will be agreed via the change control process Maximum Contract Value: £556,725 (subject to indexation)
Call-Off Contract charges	The breakdown of the Charges is held at Schedule 2 – Call-Off Charges

Additional Buyer terms

Performance of the Service	This Call-Off Contract will include the following: • Implementation Plan • Delivery of all items included in Schedule 1: Services and will be G-Cloud Services the Supplier is capable of providing through the Platform • Exit and offboarding plans and milestones
Guarantee	Not used
Warranties, representations	Not used
Supplemental requirements in addition to the Call-Off terms	Not used

Alternative clauses	Not used
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not used
Personal Data and Data Subjects	See Schedule 7; including Annex 1
Intellectual Property	Clause 7 of the G Cloud 13 supplier terms refer: 7 INTELLECTUAL PROPERTY RIGHTS 7.1 The Customer shall own all rights, title and interest in and to all the Customer Data. 7.2 The Supplier's Background IPRs shall (as between the Customer and the Supplier) be owned by the Supplier. 7.3 IPR Claims do not cover Resold Services over and above and, without prejudice to Clause 4.1 of these Supplier Terms, all references to Services in CO-11.5 shall mean Supplier Services. Clause 4.1 The Resold Services are provided subject to the service descriptions, characteristics, service levels, information security measures, terms of use and rights and remedies set out by the Resold Services Providers.
Social Value	See Schedule 1, Functional/Non Functional Requirements.

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

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

Signed	**Supplier**	**Buyer**
Name	REDACTED	REDACTED
Title	Director	Head of Commercial
Signature	REDACTED	REDACTED
Date	REDACTED	REDACTED

Customer Benefits

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

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

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

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

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

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

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

2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

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

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

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoices under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

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

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

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

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

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

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

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

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

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

15. Open source

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

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.#

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
- 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

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

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

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

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

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

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1	the activities they perform
29.2.2	age
29.2.3	start date
29.2.4	place of work
29.2.5	notice period
29.2.6	redundancy payment entitlement
29.2.7	salary, benefits and pension entitlements
29.2.9	employment status
29.2.9	identity of employer
29.2.10	working arrangements
29.2.11	outstanding liabilities
29.2.12	sickness absence
29.2.13	copies of all relevant employment contracts and related documents
29.2.14	all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as

reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

1) The Suppliers G-Cloud Service Offering is attached:

Vision-ERP_Service_
Definitinon_031223.p

2) The Supplier will provide services to the Authority as detailed below as part of the G-Cloud Clarification Process for functional and non-functional requirements

2.1) Functional/Non Functional Requirements:

Support, Change & Maintain the Insolvency Service instance of Unit4 ERP 7				Supplier Responses			
				Please mark your selection from the two options below with an 'X' in the relevant box.		If you cannot provide this, then what is the work around or future strategy?	Further Comments
#	Category	Requirement	Further Information	We can provide this	We cannot provide this		
1	**Service Provided**						
1.01	Service Provided	The supplier shall be the application development partner for The Customer.		X			Vision ERP employ expert consultants with specialisms across all modules who are more than capable of working in partnership to develop your system.
1.02	Service Provided	The supplier shall build and maintain a knowledgebase / catalogue of all the INSS bespoke configuration/set up		X			As a rule, we document any developments and fixes. These document can be added to the knowledge base, along with any other useful information we have
1.03	Service Provided	The supplier will maintain the existing configuration on the Unit 4 ERP platform.		X			Vision ERP is a partner of Unit4 and work closely with them.
1.04	Service Provided	The supplier shall document all aspects of the system to ensure a smooth transition on to the new support partner (if required at contract end).		X			We will document any developments or fixes we deploy. It is expected that existing configuration document already exist for the system in it's current state, and we will either update these as live documents or provide supplementary documentation for any work we undertake.

1.05	Service Provided	The supplier will work in collaboration with the SIAM partner, ERP hosting provider and the OSM team to provide support to the agency when it comes to Incident, Problem and Change resolution and when the agency requires.			X			Vision ERP is happy to work with other providers to ensure we are delivering the best possible service for our customers.
1.06	Service Provided	The supplier will maintain the existing email communications and alerts sent from Unit 4 ERP to internal users and external customers	Intelligent/Event setup - Purchase Orders, workflow notifications, remittances, letters		X			We can monitor these and troubleshoot issues when they occur
1.07	Service Provided	The supplier shall offer dedicated customer support, providing necessary skills and expertise to support with incident, problem and change resolution.			X			Our VRS service ensures there is a helpdesk which is accessible for our customer's operating hours. Our processes ensure that issues are logged, analysed and resolved as quickly as possibly by the best available consultant.
1.08	Service Provided	The supplier will be provided with access to our product backlog document as part of our process for management of change resolution, the supplier will be required to provide updates to document as requested based on change resolutions requested by the Authority.			X			We can provide this as part of the administration of our Consultancy on Demand service
1.09	Service Provided	The supplier shall provide an impact assessment for configuration change			X			We provide this as a matter of course as it is a vital stage in any change. This impact assessment will be carried out in conjunction with your SMEs to ensure it is a thorough assessment.
1.10	Service Provided	The Supplier shall attend workshops for any items being progressed on the backlog where required and also attend sessions as required as part of maintenance and support of the Authority's instance of ERP			X			We can provide this as part of our Consultancy on Demand service. This would normally represent the design aspect of any solution to the development backlog issues.
1.11	Service Provided	The supplier shall provide support as required/requested of Real Time Information (RTI) expert who has the necessary skills and knowledge to manage			X			We have several qualified payroll consultants who are adept at managing the RTI process
1.12	Service Provided	The supplier shall provide detailed training material and provide training sessions where required as part of			X			This is part and parcel of our Consultancy on Demand service, specifically an element of the deployment of developments into production

		change resolution and maintain existing documentation during the life of the contract					
1.13	Service Provided	The supplier shall support all environments on Unit4 ERP for INSS	Development, SIT, Pre-production and Production (ACPT01,02,03 & Live)	X			These are the usual environments we encounter
1.14	Service Provided	The supplier will support the existing Unit 4 ERP SOAP Web Services	Phase 1 - Unit 4 ERP Soap Web Service, Phase 2 - Unit 4 ERP Soap Web Service	X			Our consultants have experience with the SOAP web services, and also the newer REST API services for integration and automation.
1.15	Service Provided	The Supplier will ensure the configuration across all environments is in sync. When configuration changes are made to environments to implement solutions that allow changes to be promoted through environments rather than configured independently		X			Different environments are often at different stages due to differing requirements and testing going on. The promotion of fixes through environments is something which is managed as part of our defect resolution or change management processes. In addition, we can assist with environment strategies and schedule copies at appropriate times.
2	**Application Support & Maintenance**						
2.01	Application Support & Maintenance	The supplier shall provide support for Incident Resolutions for Unit 4 ERP (Business World) which have been allocated to the supplier within scope of the engagement, via an agreed two step triage process (Service Desk > Supplier) using the SIAMs toolset.		X			We have worked with customers in the past where we have hooked into their incident management tool to ensure we are picking up tickets allocated to us. This won't be a problem provided we have sufficient access
2.02	Application Support & Maintenance	The supplier will be responsible for support which complies with the Software Environment strategy set by the INSS, as amended from time to time.	Get software environment strategy	X			When we onboard, we ensure our processes align with our customers' environment strategy
2.03	Application Support & Maintenance	The supplier shall liaise with Unit4 (where required) directly onbehalf of InsS.		X			We can adopt INsS as a customer on our instance of the Unit4 portal which will help with managing tickets their end. We can also build a relationship with your account manager to help resolve any issues quickly.
2.04	Application Support & Maintenance	The supplier shall develop and maintain a configuration management process which works with the Azure environment and aligns to the agency's source code control strategy which includes branching strategy and code, merge and conflict resolution.			X	Unit4 are responsible for managing their application source code. The keep this	With regards to configuration management, we can comply with any governance you have with regards to providing configuration release notes.

						in DevOps and have stringent CI/CD pipelines to allow proper releases.	
2.05	Application Support & Maintenance	The supplier shall work with the hosting provider to ensure BW provides facilities for configuration / integration testing, product release testing, user training etc.		X			These facilities should be available within the existing environment setup, but we can work with InsS and Unit4 if anything further is required
2.06	Application Support & Maintenance	The supplier will work with the hosting provider to ensure BW is flexible on managing environments (ability to have as many environments as required for testing purposes).		X			Extra environments are normally provided for at an extra cost form Unit4. We can help facilitate this.
2.07	Application Support & Maintenance	The supplier will provide management and ongoing maintenance of environments within BW.		X			We will provide this as part of our VRS service. This is often done by repotting by exception to highlight when things go wrong.
2.08	Application Support & Maintenance	The supplier will work with the hosting provider to ensure that all data is successfully backed up and also to provide the Agency with the current backup schedule.	Please provide details of the backup and restore routines for the system, including as a minimum but not limited to: • Expected timings for processing incremental backups • Expected timings for processing full backups • Recommended media options available Any failed backups should be re-run immediately to ensure full coverage and data integrity.	X			The backup and restore procedures should be provided as standard by Unit4 as part of their cloud hosting solution. We can work with Unit4 to ensure InsS is fully aware of the schedules.
2.09	Application Support & Maintenance	The supplier shall ensure that any changes are supported by the automated tests as appropriate in accordance with the INSS change control process		X			We will ensure that any changes we are responsible for are tested thoroughly before being deployed into production. We will follow our change control process and ensure it aligns with the InsS process during onboarding.

2.10	Application Support & Maintenance	The supplier shall provide detailed change notes after every version update and enhancement	These notes will detail any changes that will affect our bespoke config and development.		X			Changes after upgrades are contained within the Unit4 release notes. We regularly review these. They also form part of the testing cycle as they can highlight areas which need regression testing during an upgrade. Any changes we implement will be accompanied by full documentation of the change.
2.11	Application Support & Maintenance	The supplier shall provide detailed notes where a provision is depreciated.	These notes will detail any changes that will affect our bespoke config and development.		X			Deprecated functionality is normally highlighted in the Unit4 release notes. We regularly review these and we can provide guidance to InsS if something in use it to be retired.
2.12	Application Support & Maintenance	The supplier will have a code management and release process	This will adhere to any process in CTS and will have clearly defined boundaries.		X			In terms of Unit4, there is not so much a code management release process; this is managed internally by Unit4's development team and as InsS are taking a SaaS solution, that process is a black box to InsS. However, for any configuration changes we make to the system as part of a defect or an enhancement, we will follow our standard process which will be aligned to InsS during the onboarding phase.
2.13	Application Support & Maintenance	The supplier shall ensure a support model is in place to support the unit4 ERP INSS configuration, for system issues and bug fixes not able to be resolved by OSM or Unit4 patching.			X			Normally, in a situation where an issue cannot be resolved by Unit4 patching, we work with our customers to provide an acceptable workaround. We then support this workaround and monitor release notes to ensure it still needs to be in place in case the underlying issue is fixed in a later release.
2.14	Application Support & Maintenance	The supplier shall provide full fix, test (including functional testing), release management for Unit 4 ERP using product best practice guidance and in line with agency standards.			X			Our processes conform to ITIL industry best practice processes, and we will make sure these align with InsS processes during the onboarding phase.

3	**Upgrades**						
3.01	Upgrades	The supplier shall monitor for and manage upgrades/amendments for Unit 4 ERP		X			We regularly review release notes as they come out and use them to inform any testing which might need to be done for new versions.
3.02	Upgrades	The supplier shall ensure BW is regularly updated to the latest version (N) and ensure INSS are at a minimum on version N-1.		X			With a SaaS solution, Unit4 put out a calendar for regular updates ensuring customers are always on the latest version. Normally non-production environments are updated first to give an opportunity to test, with the production environment following on shortly after
3.03	Upgrades	The supplier shall provide an impact assessment for each upgrade and changes required (including year end) to the existing software for Unit 4 ERP.	A copy of the Impact Assessment to be sent to the nominated Service Delivery Manager Check and interpret release notes and apply to INSS instance of BW. Include OSM.Team mailbox - may need support from supplier (OSM)	X			The release notes provide the changes, and from this we can provide an impact assessment. This often informs the scope of regression testing.
3.04	Upgrades	The supplier shall offer a window of support following any major changes.	Window to be defined per change (size dependant)	X			Support will be provided via our VRS service. Any support required from changes via Consultancy on Demand (e.g. backlog enhancements) are supported as part of that package and transitioned to the VRS for BAU support.
3.05	Upgrades	Modification to Unit 4 ERP made by either the hosting provider or the supplier shall be made available to the Agency within the agreed timescales and with sufficient time for testing and implementation.		X			We can provide changes made by ourselves. The Unit4 changes are out of our hands to a certain extent, but we work with UInit4 to ensure we have a timetable for when changes are coming
4	**Configurability**						
4.01	Configurability	The supplier shall be capable of configuring Unit 4 ERP in-line with INSS Business Processes		X			Our consultants are experts in configuring Unit4 ERP. They will bring a wealth of experience and best practice knowledge which InsS can make use of to guide their system developments.

4.02	Configura-bility	The supplier shall be capable of configuring Unit 4 ERP in-line with INSS Business Rules			X			Our consultants are experts in configuring Unit4 ERP. They will bring a wealth of experience and best practice knowledge which InsS can make use of to guide their system developments.
4.03	Configura-bility	The supplier shall be capable of configuring Unit 4 ERP's User Interface in-line with INSS needs			X			Where configuration of the interface is permitted by Unit4, our consultants are more than capable of ensuring it meets InsS' needs. Workspaces and dashboard provide the ultimate in UI configuration within the system, and we can develop this for InsS to meet your requirements.
5	**Reporting**							
5.01	Reporting	The Supplier shall provide reports as part of the monthly service reporting pack. Reporting pack contents shall be agreed during service establishment and periodically reviewed. It is expected that the Supplier will have a standard set of reports available.			X			We can provide reports on a monthly basis on progress. This will rely on metrics from the ticketing system at the core of the shared SIAM ecosystem
5.02	Reporting	The Supplier shall provide a copy of the monthly licencing report to the Authority's SIAM Service Integrator to inform their Software Asset Management function undertaken by the SIAM Lead Service Provider.			X			We can liaise with InsS and Unit4 to agree content of the report and provide it as required.
5.03	Reporting	The supplier shall provide a monthly report on any days used for enhancements or for call off purposes.			X			We can produce and automate this report form our own Unit4 ERPx solution
5.04	Reporting	The Supplier will ensure the current set of Management Information reporting within Unit 4 ERP is supported as per the Agency's needs			X			Our consultants have expert report writing capabilities. We will work to understand your reporitng requirements and the existing suite of reports in place to meet said requirement so that we can effectively support them.
6	**Integration**							
6.01	Integration	The supplier shall maintain the Unit 4 ERP integration with cloud-based identity management solutions for the purpose of user authentication and management.			X			IDS server configurations in Unit4 cloud is managed by the Unit4 cloud team. Vision ERP can liaise with Unit4 for InsS to ensure the integration is maintained. We will also set prompts in line with your security to remind you to generate new certificates for Unit4 to use to ensure that connections are maintained for end-users. We will need to understand your IDS setup as part of the onboarding.

6.02	Integration	The supplier shall maintain the Unit 4 ERP desktop and web version's single sign on capability with the INSS Azure Active Directory			X			IDS server configurations in Unit4 cloud is managed by the Unit4 cloud team. Vision ERP can liaise with Unit4 for InsS to ensure the integration is maintained
6.03	Integration	Unit 4 ERP shall allow system data and application services to be accessed and invoked by third party systems, including support for synchronous, a-synchronous and batch messaging structures.			X			In cloud, system data is not directly accessible (i.e. straight to database). This is normally managed by either file transfers, ora ccess via web services (SOAP or REST API). Vision ERP can support this
7	**Usability**							
7.01	Usability	The supplier shall be capable of customising the Intel Agent functionality within Unit 4 ERP to provide meaningful warning messages, help messages and to improve the user experience.			X			Configuration of IntellAgents is well within the capability of our consultants. This is a system standard tool with many uses
7.02	Usability	The supplier will undertake periodic maintenance and troubleshooting of the Intel Agent functionality within Unit 4 ERP to ensure it is working efficiently.			X			Any issues with IntellAgent can be logged as tickets for our analysts to resolve via our VRS. In addition, certain alerts can be set up to warn when there are errors with particular events.
7.03	Usability	The supplier will work with the hosting provider to ensure the Unit 4 ERP web version shall be browser agnostic	Details of the browser and versions tested should be provided			X	Unit4 product development are the ones who will drive web browser compatability. They work with all industry standard browsers including Microsoft Edge and Google Chrome. InsS should ensure that they make use of one of these	This is completely within Unit4's product development remit and there would be very little influence that anyone from outside would be able to exert. I would question anyone who thinks otherwise. We can incorporate a routinely check in line with your IT policies to assess the compatibility of Unit4 web on staged versions of your web browsers to ensure that an upgrade of your browser doesn't cause Unit4 web to not function.

							widely used and recog-nised web browsers.	
7.04	Usability	The supplier will work with the hosting provider to ensure the browser based method shall be in accordance with W3C standards				X	Unit4 should as standard work with W3C standards when im-plement-ing their web based UI. This is not within any-one's con-trol to in-fluence other than Unit4 product develop-ment.	Unit4 is currently W3C compliant and supports WCAG2.1. This is a responsibility of Unit4 to maintain. If we find that a version of Unit4 is not compatible with W3C standards, we can raise this with Unit4 on the Agen-cies behalf.
8	**Performance**							
8.01	Perfor-mance	The supplier will ensure that any changes introduced do not negatively impact the performance of Unit 4 ERP			X			All of our solutions will be thoroughly tested before de-ployment to production, which includes an aspect of performance testing.
8.02	Perfor-mance	The supplier shall provide agreed daily/weekly/monthly performance re-ports to be agreed during service tran-sition			X			Performance reporting can be agreed in the onboard-ing phase as to the source of data and content of the reports.
8.03	Perfor-mance	The supplier will highlight where Unit 4 ERP does not meet system KPIs and provide guidance to support with inci-dent response and management.			X			This is dependant on agreeing the KPIs and us being able to get to the source of the data to inform them.
9	**Manageability**							

9.01	Manageability	The supplier shall monitor response times and provide alerts if agreed thresholds are breached			X			Response times will be logged in our ticket system. If we integrate into the SIAM ticket system then we would expect that these metrics would be provided from there for us to monitor against.
9.02	Manageability	The supplier shall monitor response times and shall be expected to respond to alerts from the SIAM provider within the agreed SLA's			X			Response time monitoring will form part of the customer care package within our VRS.
9.03	Manageability	The supplier shall provide log error messages which supply sufficient information to aid problem resolution			X			These will be available from the Unit4 ERP for processes. Anything requiring extra logging such as database traces or web logs will need to be obtained from Unit4 cloud. We have the capability to do this via our partner portal.
9.04	Manageability	The supplier will provide documentation (user manuals, help guides and technical documentation) for any new configuration or bespoke changes made to Unit 4 ERP. These shall be complete and kept up to date throughout the life of the contract	Government functional standard 005		X			Vision ERP provide full documentation for any configuration changes made as a matter of course.
10	**Enhancements & Changes**							
10.01	Enhancements & Changes	The supplier shall implement, support and maintain operational enhancements as part of Continual Service Improvement to Unit 4 ERP as defined by, agreed with and signed off by the relevant business areas			X			Our expert consultants will be able to come up with best practice solutions to items raised under the banner of continuous improvement. These should follow the change management process within our Consultancy on Demand service to ensure they are designed, bult, tested, implemented and documented correctly.
10.02	Enhancements & Changes	The supplier shall ensure a minimum of 5 days of enhancement time are allocated per month to address enhancements to Unit 4 ERP. Any days not used shall be carried into the following months up to REDACTED per contract year.	Where a statement of work is required, the time taken to create will not be taken out of the enhancement days.		X			We can agree up front a call off package of work for our consultancy on demand service to cater for this.
10.03	Enhancements & Changes	The supplier shall provide a proposal including deliverables, milestones and payment criteria for any engagement seen as an enhancement within 10 working days of submission.			X			This will fit with our standard Statement of Work process whereby we gather requirements, work out a package of work, and then play this back to customers by way of a document.
11	**Recoverability**							

11.01	Recoverability	The supplier shall work with the hosting provider to ensure that recovery shall facilitate the full restoration of services within 24 hours of an incident			X			Unit4 cloud provide this service, and we can work with them in the event of an emergency to ensure swift resumption of services
12	**Governance**							
12.01	Governance	The Supplier shall attend a Quarterly Supplier Relationship Management Meeting with the Authority's named contact within CTS Service Governance and other relevant Key Stakeholders.			X			This is a standard function as part of our VRS
12.02	Governance	The Supplier shall be expected to continually improve the way in which the required Services are delivered throughout the Contract duration.			X			As part of our Relationship Management meetings, we will identify areas which work well and areas which need improvement, and continuously aim to improve our services.
12.03	Governance	If the Supplier identifies further opportunities and new ways of working that could be exploited these should be presented to the Authority during regular Relationship Management meetings, and in accordance with Schedule 3 (Continuous Improvement)			X			Continuous improvement is baked into our service offering
12.04	Governance	Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.			X			Changes will be identified and agreed via the Relationship Management meetings prior to any implementation
12.05	Governance	The Supplier shall contribute to the CTS Continual Service Improvement Register as part of the Relationship Management Meeting.			X			Continuous improvement is baked into our service offering
12.06	Governance	The supplier shall contribute to the CTS Operational Risk Register as part of the Relationship Management Meeting.			X			This should be a standing agenda item for the Relationship Management meetings
12.07	Governance	The Supplier shall participate in reviews with the Authority, to include appropriate subject matter experts. The level of engagements with Contracting Authority will be agreed within (1) month of the Call Off Contract.			X			

12.08	Governance	The Supplier shall provide a named point of contact with whom the Authority can maintain open channels of communication with to resolve issues, share lessons learned and present new ways of working during the agreed review meetings.			X			This will be Matthew Bland, our Vision Response Service Manager and Director of Existing Business
12.09	Governance	The supplier will maintain new system, service, Architecture, and integration documentation for Unit 4 ERP	All modelling published to CTS or the SIAM Ecosystem should be in ArchiMate. The IP and associated documentation to be documented in/importable into our BiZZdesign platform.		X			We will need guidance on how to fit into the formats described in cell D83
12.10	Governance	The supplier will submit changes via the Lead Service Integrator's change management process, based on ITILv3 framework, when implementing changes to live platform instances. This will ensure that changes are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented, and reviewed in a controlled manner.			X			This aligns to our change management process, and we will be able to integrate it seamlessly with InsS in the SIAM ecosystem.
12.11	Governance	The supplier shall adhere to agreed SLAs			X			
12.12	Governance	All Incidents shall be classified to one of the following four severity levels: All Incidents shall be classified to one of the following four severity levels: • P1 • P2 • P3 • P4			X			These are our standard priority levels
12.13	Governance	A P1 classified incident shall meet the following response/resolution times: - • Response time 15 mins • Resolution 4 Business Hours			X			This is in line with our standard SLA
12.14	Governance	A P2 classified incident shall meet the following response/resolution times: - • Response time 30 mins • Resolution 8 Business Hours			X			This is in line with our standard SLA
12.15	Governance	A P3 classified incident shall meet the following response/resolution times: - • Response time 30 mins • Resolution 2 Working Days			X			This is in line with our standard SLA

12.16	Governance	A P4 classified incident shall meet the following response/resolution times: - • Response time 30 mins • Resolution 4 Working Days		X			This is in line with our standard SLA
12.17	Governance	Supplier shall supply new or enhanced services within the agreed timescale set out at commencement of the task.		X			
12.18	Governance	Supplier shall supply proposals for new or enhanced services within the agreed timescale set out at commencement of the task.		X			
12.19	Governance	All Service Requests shall be classified to one of the following three severity levels: • P1 • P2 • P3		X			This is 1 level fewer than our standard set, but we can adapt to meet this
12.20	Governance	A P1 request is classified as requiring a fulfilment target of 2 working days		X			This is in line with our standard SLA
12.21	Governance	A P2 request is classified as requiring a fulfilment target of 3 working days		X			This is in line with our standard SLA
12.22	Governance	A P3 request is classified as requiring a fulfilment target of 5 working days		X			This is in line with our standard SLA
12.23	Governance	Supplier shall meet an availability service level target of 99.9%		X			We have sufficient staff to ensure cover is in place
12.24	Governance	The Supplier shall be responsible for the provision of training for any new bespoke changes to Unit 4 ERP introduced		X			This is delivered as part of the Consultancy on Demand service as part of any changes
12.25	Governance	The Supplier shall ensure that appropriate training is provided to Contracting Authorities Users to enable effective usage of the product(s) that support service delivery		X			Additional training can be provided through our Training service as part of the VRS. Any training that would be needed as part of an enhancement will be included as per the enhacement package of work.
12.26	Governance	The supplier will attend the weekly or otherwise agreed CAB meetings		X			
13	**SIAM**						
13.01	SIAM	The supplier will sign up to the SIAM Collaboration Agreement	Full Service Provider	X			Vision ERP can sign up to this and work in collaboration with other organisations.

13.02	SIAM	The supplier will be managed as part of the SIAM EcoSystem in line with the Collaboration Agreement and work alongside all other Service Providers	Full Service Provider		X			Vision ERP works well in collaboration with other organisations, and have a longstanding relationship with Unit4, the software suppler and cloud host.
13.03	SIAM	The supplier will attend a monthly SIAM Service Review meeting with the Lead Service Provider alongside all other Service Providers	Full Service Provider		X			This is a part of our standard VRS service
13.04	SIAM	The supplier will contribute to the Continual Service Improvement Register across the EcoSystem as part of the SIAM Service Review Meeting.	Full Service Provider		X			This is a part of our standard VRS service
13.05	SIAM	The supplier will contribute to the Operational Risk Register across the EcoSystem as part of the SIAM Service Review Meeting.	Full Service Provider		X			This is a part of our standard VRS service
13.06	SIAM	The supplier will engage with the INSS' Service Governance Team to produce Rough Order of Magnitudes in terms of project and/or major changes when required.	Full Service Provider		X			This is a part of our standard VRS service
13.07	SIAM	The supplier will provide a monthly register of all assets (where applicable) to be uploaded into Remedy as part of the overall Asset Register.	Full Service Provider		X			This is a part of our standard VRS service
13.08	SIAM	The supplier will attend the weekly or otherwise agreed CAB meetings	Full Service Provider		X			This is a part of our standard VRS service
13.09	SIAM	The supplier will submit requests for change in line with the standard ITIL process via the Lead SIAM Provider	Full Service Provider		X			Vision ERP will adapt our processes to conform to the SIAM requirements
13.10	SIAM	The supplier will participate in the weekly or otherwise agreed meetings with the Lead SIAM Provider's Technical Architect	Full Service Provider		X			This is a part of our standard VRS service
13.11	SIAM	The supplier will participate in regular Supplier Relationship Management meetings with an appointed Agency Service Delivery Manager to produce regular service reports as required.	Full Service Provider		X			This is a part of our standard VRS service
13.12	SIAM	The supplier will take an active role as a Provider during Major Incidents, including attending technical bridge calls.	Full Service Provider		X			This is a part of our standard VRS service

13.13	SIAM	The supplier will be granted access to the Lead SIAM Service Provider's Remedy tool for collaborating across the EcoSystem for the management of assigned incidents, requests, problem and change tickets. For access to this system the supplier will require a user licence.	Full Service Provider	X			This is a part of our standard VRS service
13.14	SIAM	The supplier will comply with standard authentication and identification methods in use for INSS applications for end-users and administrative support purposes.	Full Service Provider	X			Vision ERP is fully equipped to comply with the standard authentication and identification procedures for both end-user and administrative applications. We employ a robust identity management framework that ensures secure access control and identity verification, in line with industry best practices. This framework is regularly updated to respond to emerging security threats and to adhere to the latest standards in identity management.
14	**Supplier Personnel**						
14.01	Supplier Personnel	The Supplier shall ensure that all Supplier Personnel possess the qualifications, experience and competence appropriate to the tasks for which they are employed		X			We put all our resources through vetting as part of their onboarding, and will ensure that we match the skills of the resources to the tasks in hand. All our Unit4 resources are committed to obtaining their Unit4 accreditations which helps them demonstrate the application knowledge along with their experiences.
14.02	Supplier Personnel	The Supplier shall ensure that all Supplier Personnel delivering the Product Range to Contracting Authorities are fully trained for the work they are undertaking and have direct access to the manufacturer's current technical manuals and support services		X			All of our Unit4 resources undergo Unit4 training which is part of onboarding, and continuous as part of their development plans. This enables our workforce to hold Unit4 accreditations in various specialties of the system. Where accreditations are not available, we ensure all resuorces are up-to-speed with the latest developments and best practise to enable them to carry out their duties effectively.
14.03	Supplier Personnel	The Supplier shall ensure that all Supplier Personnel adhere and comply with Contracting Authorities' safety and confidentiality requirements are met at all times		X			We will ensure that all resources are fully aware of the safety and confidentialit requirements. We will need to ensure that any updates to these requirements are shared with us so we can keep our team's knowledge up-to-date.
14.04	Supplier Personnel	The Supplier shall ensure that all Supplier Personnel supplying the Services shall act in a responsible and professional manner, and shall provide and maintain the Product Range with all due skill, care and diligence		X			We will ensure that all personnel used for the Agency act in professional and resposible manner. We constantly review our quality control processes to ensure that all resources comply.

14.05	Supplier Personnel	The supplier shall ensure that a Baseline Personnel Security Standard (BPSS) is undertaken for all supplier personnel and any subcontractors before any work is undertaken			X			We will ensure that BPSS is undertaken by all personnel and subcontractors. Please also be advised that all personnel hold SC clearances.
14.06	Supplier Personnel	The supplier shall ensure that a Security Check (SC) is undertaken for all supplier personnel who have access to significant amounts of INSS data before any work is undertaken	The Authority reserves the right to mandate SC Clearance where deemed appropriate in accordance with Government Security Classification May 2018.		X			All of our resources will currently hold SC clearances. We will comply with additional screening should it be needed.
14.07	Supplier Personnel	The Supplier shall ensure that all Supplier Personnel have appropriate security clearance and comply with any additional security requirements specified by Contracting Authorities			X			All of our resources will currently hold SC clearances. We will comply with additional screening should it be needed.
15	**Availability**							
15.01	Availability	The supplier shall provide procured service between Mon - Fri, 7:00 to 19:00 excluding UK Public Holidays			X			We will be able to provide support between 7:00 - 19:00, Mon-Fri. We can also offer support outside of this time for critical issues, or pre-planned deployments.
15.02	Availability	The supplier will pro-actively manage and report on availability of BW's uptime on behalf of the hosting provider against agreed capacity levels			X			We will work with Unit4 to ensure a robust practise in enforced to notify us should the agreed capacity levels are not adhered to.
15.03	Availability	The supplier shall provide specialist functional support in order to configure the software to allow the Agency to meet the changing needs of the business such as process development, policy change and organisational restructures. It will be the supplier's responsibility to ensure the data integrity and confidentiality are preserved at all times.			X			We will be able to use our expertise and experience to configure the software to meet changing needs of the business. We will ensure we keep data integrity and confidentiality preserved at all times.
16	**Audit**							
16.01	Audit	The supplier shall shall provide a full BW audit history to include user name, date and time stamp at field level on data items as agreed with INSS upon request	Responses should indicate how long audit logs are retained for.		X			We will use amendment logging along with login sessions to provide audit history. We will need to ensure that we are logging and monitoring the correct data tables as agreed with INSS.
16.02	Audit	Audit history shall be fully reportable with the ability to detail all user and system touch points at transaction level.			X			We will ensure that full audit history is available at transactional level.

16.03	Audit	Where applicable, throughout BW, the supplier shall track and monitor all software asset usage.			X			We will be able to monitor software usage. Session history is available to see who has logged on.
16.04	Audit	All maintenance activities carried out shall be logged and auditable			X			We will keep a log of all maintenance activities. This will include vendor planned activities and our activities.
16.05	Audit	The supplier will facilitate the integration of the BW Audit logs into the INSS' Security Operating Centre (SOC)			X			We will facilitate the integration of the Audit logs into INSS SOC.
17	**Performance**							
17.01	Performance	The supplier will ensure that any changes introduced do not negatively impact the performance of BW			X			We will ensure that thorough testing is carried out in "like-production" environments to ensure that performance is not negatively impacted.
17.02	Performance	The supplier shall provide agreed daily/weekly/monthly performance reports to be agreed during service transition			X			We will work with the agency to set out the most appropriate method and frequency of reporting performance. We will factor this in our service transition period. We will work with Unit4 to obtain performance related metrics.
17.03	Performance	The supplier shall work with the hosting provider to ensure BW is performant in-line with published performance metrics			X			We will work closely with Unit4 to ensure that performance is in-line with published metrics.
17.04	Performance	The supplier will highlight where BW does not meet KPIs and provide guidance			X			We will highlight where KPI's are not being met. As part of the onboarding, please provide us the KPI's
18	**Environment & Sustainability**							
18.01	Environment & Sustainability	The Supplier shall comply with Government Buying Standards.	Full details of which can be found on the DEFRA Sustainable Development in Government website: https://www.gov.uk/government/publications/government-buying-standards		X			We are fully compliant with the Government Buying Standards, ensuring that our procurement practices prioritize sustainability and efficiency. We regularly review our processes to align with the latest DEFRA guidelines.
18.02	Environment & Sustainability	The Supplier shall complete annual Corporate Social Responsibility (CSR) assessments						We will conform with CSR assessments.

18.03	Environment & Sustainability	The Supplier shall comply and operate to the standard ISO 14001; Eco-Management and Audit Scheme (EMAS) or a nationally recognised agreed equivalent accredited standard for the scope of the Product Range			X			We maintain compliance with ISO 14001, demonstrating our commitment to environmental management. Our operations are regularly audited to ensure adherence to this internationally recognized standard.
18.04	Environment & Sustainability	The Supplier shall work co-operatively and provide assistance to Contracting Authorities to support the Government's Agenda to meet the Greening Government Commitments (GGC), including associated reporting requirements	Full details can be accessed via the following link https://www.gov.uk/government/collections/greening-government-commitments		X			We work collaboratively with Contracting Authorities to support the GGC, providing assistance and adapting our practices to meet the UK Government's sustainability goals. We have implemented measures to ensure our reporting aligns with the required environmental standards. We are a small company and where possible we work remotely, and dispose of any redundant IT equipment in an environmentally fashion.
19	**Accessibility**							
19.01	Accessibility	The supplier will highlight to the Agency how the BW desktop version can conform to agreed accessibility standards upon request			X			We can assess this and provide some options on accessibility. The more robust solution is to use the web interface which confirms to WCAG2.1.
19.02	Accessibility	The supplier will highlight to the Agency how the BW web version can conform to Web Content Accessibility Guideline (WCAG) upon request	https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag		X			We can confirm that unit4 web conforms to WCAG2.1. We will keep updated with any developments with standard changes and re-assess if Unit4 is still compliant.
20	**Security**							
20.01	Security	The supplier shall provide relevant support to the Agency in relation to any potential security breaches of the solution.			X			We have a robust incident response plan that aligns with industry best practices to support the Agency in any potential security breaches of the solution.
20.02	Security	Roles and responsibilities between all parties around data losses shall be documented and agreed upon in advance of the contract signing.			X			Responsibilities and protocols for data loss prevention and response are clearly documented and reviewed regularly in partnership with all parties.
20.03	Security	The supplier will assist the Agency and associated third parties where we have the right to undertake penetration testing of Unit 4 ERP periodically			X			Our processes fully support external audits by authorised parties, ensuring transparency and cooperation in security matters.

20.04	Security	The supplier shall ensure that data is only extracted from Unit 4 ERP with the Agency's approval		X			We ensure strict data isolation between Unit4 ERP and the Agency's data systems through encrypted channels and access controls.
20.05	Security	The supplier shall track and monitor all Unit 4 ERP related hardware and software asset usage on behalf of the Agency		X			Procedures are in place to ensure that any data exported from Unit4 ERP on behalf of the Agency is done securely, adhering to the Agency's asset management protocols.
20.06	Security	The supplier will provide the Agency with information regarding security vulnerabilities detected within Unit 4 ERP	This information should be available centrally and please provide further details of the Unit 4 ERP's ability to cascade the information to a configurable endpoint of our choosing.	X			We provide timely information on vulnerabilities, enabling the Agency to apply necessary measures to the ERP system's security posture.
20.07	Security	Throughout Unit 4 ERP the supplier shall demonstrate separation of duties to ensure that any damage/loss caused by a malicious internal threat actor will be limited		X			Our architecture ensures complete data separation, preventing any cross-contamination and securing data integrity.
20.08	Security	Throughout Unit 4 ERP the supplier shall provide adequate separation of users, data and systems to protect both data and infrastructure from malicious or authorised activity.		X			We uphold stringent measures for authorised separation of users, data, and processes to maintain security integrity across all operations.
20.09	Security	If the supplier decides to use a 3rd party specialist functional support team to support the Unit 4 ERP platform in order to meet the changing needs of the business such as process development, policy change and organisational re-structures – It is down to the supplier to ensure that the Integrity and confidentiality of the data is preserved.		X			Our ERP system is designed for adaptability to changing needs, with a focus on security-first development and policy compliance.
20.10	Security	The supplier shall provide evidence of adhering to the NCSC cloud security principles.	https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles	X			We adhere to the NCSC cloud security principles, ensuring our cloud deployments meet the highest standards of security.
20.11	Security	The supplier shall adhere to the principles in the Government Functional Standard GovSec007.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016424/GovS_007-_Security.pdf	X			Our security measures align with the government security classification policy, safeguarding sensitive information effectively.
20.12	Security	The supplier shall adhere to the Government Security Classification policy	https://www.gov.uk/government/publications/government-security-classifications	X			Compliance with the Government Security Classification Policy is integral to our operation, with regular training and audits to maintain adherence.

20.13	Security	The supplier shall adhere to the guidance issued by the Centre for Protection of National Infrastructure on Risk Management	https://www.cpni.gov.uk/content/adopt-risk-management-approach	X			We follow a risk management approach consistent with the Government's standards, ensuring a proactive stance on security threats.
20.14	Security	The supplier shall adhere to the Accreditation of Information Systems	https://www.cpni.gov.uk/protection-sensitive-information-and-assets	X			Our information systems accreditation process follows rigorous standards, guaranteeing secure and reliable operations.
20.15	Security	The supplier shall adhere to the National Cyber Security Centre's (NCSC) information risk management guidance	https://www.ncsc.gov.uk/collection/risk-management-collection	X			We comply with the NIS regulations, ensuring our network and information systems meet required security standards.
20.16	Security	The supplier shall adhere to the Cyber Essentials / Cyber Essential Plus for Internet facing solutions	https://www.ncsc.gov.uk/cyberessentials/overview	X			We maintain Cyber Essentials certification and regularly review our cyber security measures to align with evolving standards.
20.17	Security	The supplier shall ensure all Standards set out in the Minimum Cyber Security Standards document are met, specifically sections 6 & 7	https://www.gov.uk/government/publications/the-minimum-cyber-security-standard	X			Our security controls exceed the Minimum Cyber Security Standards, with an ongoing commitment to cyber resilience.
20.18	Security	The supplier shall complete and provide a Data Privacy Impact Assessment	https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf	X			We conduct thorough Data Privacy Impact Assessments for all new and existing systems, ensuring compliance with data protection regulations.
20.19	Security	The supplier shall be evidence compliance with a recognised Information Security Management System (ISMS), for example ISO27001:2013, NIST, CSA GoldStar	https://www.iso.org/standard/54534.html	X			Our ISMS is certified against ISO/IEC 27001:2013, demonstrating our commitment to international best practices in information security management.
20.20	Security	The supplier shall be compliant with ISO27018:2014	https://www.iso.org/standard/61498.html	X			We comply with ISO/IEC 27018:2014, protecting personal data processed in our cloud services and upholding the privacy of individuals.
20.21	Security	The supplier shall be compliant with the Cabinet Office's 15 good practice measures for the protection of bulk data held by digital services	https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main	X			Our cloud services adhere to G-Cloud 15's good practice measures, ensuring secure and compliant cloud solutions.

20.22	Security	The supplier shall be compliant with the SaaS Security Principles	https://www.ncsc.gov.uk/collection/SaaS-security/SaaS-security-principles	X			We align with the SaaS Security Principles, ensuring secure software-as-a-service offerings through continuous security assessments.
20.23	Security	The supplier shall adhere to the Government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint	https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice	X			Our digital services are designed and maintained in accordance with the Digital Service Standard, ensuring a secure and user-focused delivery.
20.24	Security	The supplier shall adhere to the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance	https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles	X			We operate in strict compliance with the Cloud Security Principles, providing secure and resilient cloud services.
20.25	Security	The supplier shall have a clearly defined and documented security governance framework which will include a security incident response plan.	Further Guidance Please provide details as to your response. Holding an industry standard certification such as ISO 27001 would be beneficial.	X			Our security governance framework is comprehensive, documented, and includes an incident response plan, aligning with standards like ISO 27001. We have the auditable documentation in place, and are currently going through the accreditation process for this.
20.26	Security	The supplier shall provide a Data Loss Prevention Strategy	There must be a robust data loss prevention strategy in place. Supplier must work with the Agency to create and maintain the DLP strategy.	X			We will work with the agency to produce a robust Data Loss Prevention Strategy
20.27	Security	The supplier will meet the OWASP ASVS standard	https://owasp.org/www-project-application-security-verification-standard/	X			Our application development adheres to OWASP standards, ensuring the security of our web applications against common vulnerabilities.
20.28	Security	The supplier shall ensure that any SQL and application patches, updates, upgrades are applied in accordance with the Agency's patching standards, as amended from time to time (as set out attached vulnerability policy)		X			Our patch management process is robust, with updates and upgrades managed in accordance with the Agency's standards. This will relate to the ERP application hosted by Unit4. We will liaise with both Unit4 and the Agency to ensure we know when the latest product updates are being deployed so we can prepare for testing.
20.29	Security	The supplier will ensure any data in non-live environments is regularly updated and pseudonymised		X			We ensure that non-live environments are updated and secured to the same standards as live environments to prevent any security risks.

20.30	Security	The supplier will not be granted access to live Unit 4 ERP data unless specifically agreed by the Agency			X			We restrict access to Unit4 ERP data to authorised personnel only, with regular reviews to ensure ongoing compliance and security.
21	**Legal**							
21.01	Legal	The supplier must comply with the The Electronic Communications Act 2000	https://www.legislation.gov.uk/ukpga/2000/7/contents		X			We have an established compliance framework ensuring all electronic communications are conducted in line with the Electronic Communications Act 2000, including regular audits and staff training programs.
21.02	Legal	The supplier must comply with the The Regulations of Investigatory Powers Act 2000	https://www.legislation.gov.uk/ukpga/2000/23/contents		X			Our operations fully comply with RIPA 2000 requirements. We have strict protocols for surveillance and data interception, overseen by a designated compliance officer.
21.03	Legal	The supplier must comply with The Terrorism Act 2006	https://www.legislation.gov.uk/ukpga/2006/11/contents		X			We adhere to the Terrorism Act 2006 through rigorous checks and risk assessments, ensuring no support is given to terrorism-related activities.
21.04	Legal	The supplier must comply with The Police and Criminal Evidence Act 1984	https://www.legislation.gov.uk/ukpga/1984/60/contents		X			Compliance with PACE 1984 is integral to our operations. We have clear procedures for the protection and handling of evidence and information.
21.05	Legal	The supplier must comply with The Computer Misuse Act 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents		X			Our cybersecurity policies are designed to comply with the Computer Misuse Act 1990, including regular IT security training and system audits.
21.06	Legal	The supplier must comply with The Public Records Act 1958	https://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents		X			We maintain compliance with the Public Records Act 1958 through meticulous record-keeping and archiving processes.
21.07	Legal	The supplier must comply with The Official Secrets Act 1989	https://www.legislation.gov.uk/ukpga/1989/6/contents		X			All employees undergo vetting and sign confidentiality agreements to comply with the Official Secrets Act 1989.
21.08	Legal	The supplier must comply with The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2000/36/contents		X			We uphold the Freedom of Information Act 2000, with a transparent information request process managed by our dedicated FOI team.

21.09	Legal	The supplier must comply with the EU Network and Information Security directive and regulations 2016	https://www.legislation.gov.uk/uksi/2018/506/made		X			Our IT infrastructure is aligned with the NIS Directive, ensuring the security of network and information systems.
21.10	Legal	The supplier must comply with any applicable code of practice produced by ombudspersons, such as the Parliamentary and Health Services (PHSO) or Information Commissioner (ICO)	https://www.ombudsman.org.uk/		X			We follow best practice guidelines from ombudspersons like the PHSO and ICO to uphold our commitment to service excellence and information security.
21.11	Legal	The supplier will maintain that Unit 4 ERP is compliant with the International Audit & Accounting standards	https://www.iaasb.org/publications/2021-handbook-international-quality-control-auditing-review-other-assurance-and-related-services		X			Our financial reporting is in line with International Audit & Accounting Standards, as verified by external audits.
22	**Social Value**							

Guidance:
The Public Sector is a major market player across a variety of spend areas and has considerable influence on the markets it operates in and as a result the Buyer has an opportunity:
• To maximise benefits effectively and comprehensively through Public Sector commercial activity.
• Have a lasting impact on individuals, communities and the environment. Social Value creates the potential to release millions of pounds of public money for community benefit.
• To encourage smarter spending to not only deliver a proposed service but also address social, economic and environmental issues in the local community.
• To help drive innovation, drive out inequalities, bring communities together, connect people with the environment and improve health & wellbeing.

This aligns to Central Government's National Procurement Policy Statement and its commitment to taking account of Social Value in procurement activity. The Buyer has selected the following Government Social Value themes to evaluate as part of this tender.

22.01	Social Value	Please describe your current or planned activities towards: Social Value Theme 2: Tackling Economic Equality - Support the development of scalable and future-proofed new methods to modernise delivery and increase productivity.	A response will include activities that demonstrate and describe the tenderer's existing or planned: Understanding and creation of scalable and future-proofed new methods to drive greater modernisation of delivery and increase productivity. Illustrative examples of creation of scalable future proofed methods include: • Outcome based specifications enabling alternative approaches to be offered; co-designed by users and communities; • Approaches that invite innovative proposals to be considered and developed; • Activities that promote collaboration to access new and green technologies and approaches • Approaches to organisational learning and continuous improvement.			REDACTED.
22.02	Social Value	Please describe your current or planned activities towards: Social Value Theme 4: Equal Opportunity - Demonstrating action to identify	A response will include activities that demonstrate and describe the tenderer's existing or planned:			REDACTED

		and tackle inequality in employment, skills and pay in the contract workforce.	Understanding of the issues affecting inequality in employment, skills and pay in the market, industry or sector relevant to the contract, and in the tenderer's own organisation and those of its key sub-contractors. Measures to tackle inequality in employment, skills and pay in the contract workforce. Illustrative examples: • Inclusive and accessible recruitment practices, and retention-focussed activities. • Offering a range of quality opportunities with routes of progression if appropriate, e.g., T Level industry placements, students supported into higher level apprenticeships. • Working conditions which promote an inclusive working environment and promote retention and progression.		

Schedule 2: Call-Off Contract charges

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

Item	Insolvency Service Requirements	Further Details On Service Requirements	Year 1 Cost January 2024 to July 2024 (6 Months)	Year 2 Cost July 2024 to July 2025	Year 3 Cost July 2025 to July 2026	Estimated Cost Extension July 2026 to July 2027 (£)	Additional Notes
1	Provision for maintenance and support for our Instance of Unit4 ERP	Provide a fixed price for support and maintenance for our uses supporting with issues investigation and resolution and maintaining the service it delivers. Please See Appendix C Statement of Requirements for further information. **Note for Year 1 we expect this requirement for 6 months**	REDACTED				This is against our "enable" skill on the SFIA. This rate is £750 per day Indexation to be applied for Years 2, 3 and Extension year aligned to the CPI Index
2	Provision of resource for making enhancements to our Instance of Unit4 ERP	Provide pricing information for enhancement days REDACTED over a 12 month period, 5 days per month. Please See Appendix C Statement of Requirements for further information **Note for Year 1 we expect this requirement for 6 months**	REDACTED				This is against our "enable" skill on the SFIA. This rate is £750 per day Indexation to be applied for Years 2, 3 and Extension year aligned to the CPI Index.
3	Provision for SIAM Integration	Please detail pricing information for integrating with our SIAM requirement (if applicable). Please See Appendix C Statement of Requirements for further information **Note for Year 1 we expect this requirement for 6 months**	REDACTED				This is against our "Ensure/Advise" skill on the SFIA. This rate is £800 per day Indexation to be applied for Years 2, 3 and Extension year aligned to CPI Index.

4	Any Onboarding Activity	Please include any pricing detail related to onboarding activities related to our instance of Unit4 ERP (if applicable). Please See Appendix C Statement of Requirements for further information **Note for Year 1 we expect this requirement for 6 months**	REDACTED	This is against our "enable" skill on the SFIA. This rate is £750 per day
Total Cost (£)			REDACTED	Indexation to be applied for Years 2, 3 and Extension year aligned to CPI Index.

2. Pricing for years 2, 3 and the optional extension year are subject to Indexation.

3. Indexation will be applied using the Consumer Price Indexation (CPI) Consumer price inflation, UK - Office for National Statistics

4. Costs covered under Item 2 are an indication of costs based on the need for REDACTED of enhancement support, utilising this will be undertaken via a request for enhancement services commissioned via an agreed process between the Buyer and Supplier.

5. There may also be the need for additional service requested by the Buyer to the Supplier, these will be requested by the agreed commissioned process (see Point 2) and costs aligned to the SFIA Rate card.

6. The Suppliers SFIA Rate Card is attached for reference:

Vision_ERP_SFIA_Rate_Card_031223.pdf

Schedule 3: Collaboration agreement

Not used

Schedule 4: Alternative clauses

Not used

Schedule 5: Guarantee

Not used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.

Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR

Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax

Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or

	defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.

Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a 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 Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.

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

Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-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: UK GDPR Information

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

Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are:
REDACTED

1.1.1 Personal information charter - Department for Business and Trade - GOV.UK (www.gov.uk)

1.1.2 Data Protection Officer
REDACTED

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

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 16 of the following Personal Data: ● The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below. The Supplier will not store or process any personal data. The Buyer will access system configuration of the Finance data. If the Buyer has a service incident, then the Supplier may access the solution for investigation purposes. The Service processes interfaces which contain personal data (bank account and name), these are only accessible to the Supplier if the Buyer requests access and no data will be amended as part of the process. The Buyer will not be responsible for the storing or processing of any personal data.
Duration of the Processing	For the duration of the agreement but only for those specific events directed by the Buyer

Nature and purposes of the Processing	Access to be provided to data only to diagnose service incidents. No data to be amended or removed as part of that process, any data issues will be returned to the Buyer. The supplier will handle / process configuration changes only As part of development the Supplier may (at the Buyers direction): • Run reports / tests against the Buyer data • Batch interface data (no changes to the actual data)
Type of Personal Data	Name, address, date of birth, NI number, telephone number, bank account, email
Categories of Data Subject	Staff of the Buyer (including permanent, temporary, agency and volunteers), Customers, Clients and Suppliers of the Buyer.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	No data will be held by the Buyer at any time.

Annex 2: Joint Controller Agreement

Not used