Crown Commercial Service

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

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.

Digital Marketplace service ID number	152242027022542
Call-Off Contract reference	TIS0561
Call-Off Contract title	Agresso Remediation
Call-Off Contract description	Remediation of the Agresso solution
Start date	10 October 2022
Expiry date	The contractual term will be for a 14-week delivery period which must be completed by 31 March 2023 to cover this subject to actual start date of delivery. REDACTED
Call-Off Contract value	£104,985 fixed price
Charging method	Invoice
Purchase order number	Issued after contract signed

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

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

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

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

From the Buyer	Insolvency Service 3rd Floor, Cannon House 18 Priory Queensway Birmingham B4 6FD
To the Supplier	Equiniti ICS 205 Airport Road West Belfast BT3 9ED Company number: NI036763 EQICS is part of the Equiniti Group
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: REDACTED

Name: REDACTED

Email: REDACTED

Phone: REDACTED

For the Supplier:

Title: REDACTED

Name: REDACTED

Email: REDACTED

Phone: REDACTED

Call-Off Contract term

Start date	This Call-Off Contract Starts on the **10 October 2022** and is valid **until 31 March 2023**. This call-off contract shall expire on 31 March 2023**.**
Ending (termination)	The notice period for the Supplier needed for Ending the CallOff 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 fromthe 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 up to **3 months,** by giving the Supplier written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: Lot 3: Cloud support
Additional Services	None
Location	The Services will be delivered to remotely by the supplier.
Quality standards	Not used
Technical standards:	Not used

Service level agreement:	Not Used
Onboarding	Not used
Offboarding	Not used
Collaboration agreement	Not used
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed 125% of the Charges payable by theBuyer to the Supplier during the Call-Off Contract Term. The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to theSupplier during the Call-Off Contract Term. The annual total liability for all other Defaults will not exceedthe greater of 125% of the Charges payable by the Buyer tothe Supplier during the Call-Off Contract Term.

Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimumlimit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than **28** consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: Audit provisions from clauses 7.4 to 7.13 of the FrameworkAgreement apply.

Buyer's responsibilities	The Buyer is responsible for delivering the following environments: DEV, SIT1, Pre-Production, Prod Access: jointly with the Supplier (c/o Embridge Consulting) - Access to systems, and security vetting clearance in place before project can start.
Buyer's equipment	The Buyer is responsible for delivering the following environments: DEV, SIT1, Pre-Production, Prod. Buyer ISO 27001 certified. The G-Cloud Framework and Call-Off Contract shall takeprecedence.

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors orPartners and the subcontractor's partners. • Embridge Consulting (UK) Limited - Company number 09600193. • Quickthink Cloud Limited – Company number 08783872. o Referred to in the supplier's proposal as 'QTC' • Supplier to provide named Embridge Consulting (UK)Limited and Quickthink Cloud Limited personnel. • Embridge Consulting (UK) Limited will supply personnel that currently hold NPPV3 clearance. Buyer will send the named personnel Security Clearance forms for processing by the Buyer's Cyber Security team.
Supplier's responsibilities	Access: jointly with the Supplier (c/o Embridge Consulting) - Access to systems, and security clearance in place before project can start. The supplier is responsible for providing the buyer with the names of individuals that require security clearance at least 5 working days before their start date.

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 **via BACS**
Payment profile	The payment profile for this Call-Off Contract is a fixed price payable on delivery of the Agresso Remediation, as per Schedule 2 of the Call-Off Contract.

Invoice details	The Supplier will issue electronic invoices on delivery of the Agresso Remediation phase outputs. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent via email to REDACTED

Invoice information required	All invoices must include contract reference TIS0561, the current Purchase Order Number and a copy of approval/acceptance of the delivery of the Services by the Buyer.
Invoice frequency	Invoice will be sent to the Buyer on delivery of the Agresso Remediation milestone outputs as per Schedule 2 of the Call-Off Contract.
Call-Off Contractvalue	The total value of this Call-Off Contract is £104,985
Call-Off Contract charges	The breakdown of the Charges is £104,985 for delivery of the Agresso Remediation outputs, as per Schedule 2 of the Call-Off Contract. This is based on a fixed price.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the delivery of all items includes in Schedule 1: Services of this Call-Off Contract.
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

Public Services Network (PSN)	Not used
Personal Data and Data Subjects	Not used

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 Contractterms 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 signedcopy 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 (PartB) 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 underthe terms of Framework Agreement number RM1557.12.

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

Signed		
Name	REDACTED	REDACTED
Title	REDACTED	REDACTED
Signature	REDACTED	REDACTED
Date	06/10/2022	06/10/2022

Schedule 1: Services

Service definition:

https://www.digitalmarketplace.service.gov.uk/g-cloud/services/152242027022542

152242027022542-service-definition-do

Terms & Conditions:

The G-Cloud Framework and Call-Off Contract shall take precedence.

Pricing document:

152242027022542-pricing-document-20

Reason for Change: The servers and infrastructure used within The Insolvency Service's environments are running platforms/components that are past their end of life and are therefore no longer supported. This is a risk to the business.

Requirement: The Insolvency Service require that all unsupported applications are upgraded/rebuilt to a supported supplier software version.

- Recommended remediation required

Operating Systems

All Windows operating systems to be upgraded to Windows Server 2019, thereby providing a compliant and Microsoft supported operating system to September 2029.

Software	Mainstream Support End	Extended Support End
Microsoft Windows Server 2019	01/09/2024	01/09/2029

Database Platform

All instances of Microsoft SQL Server are upgraded to Microsoft SQL Server 2019.

Software	Mainstream Support End	Extended Support End
Microsoft SQL Server 2019	07/01/2025	08/01/2030

Agresso Application

The preferred approach will be to upgrade the Agresso version to the latest stable ERP version. Namely Release 7 Update 8.

Out of Scope: Please note the service management proposal, pages 138 to 145 of 146 of the supplier's proposal 07.09.22 refers, is outside of the scope of this contract and relates to contract TIS0448 Equiniti Case Management Services: Provision of a Managed Service & Upgrade Services.

Scope: The Insolvency Service have specified the underlying Operating Systems and SQL Server versions to be targeted as part of the Technology Refresh. These are:

- Microsoft Windows Server 2019
- Microsoft SQL Server 2019 (Including Reporting Services)

EQ is proposing an application level refresh of its initially provided Unit4 Agresso 5.5.0 SP2 application

Refresh Approach

Staff from Embridge Consulting and their sub-contractor QTC will lead the refresh, carrying it out in accordance with their proven and repeatable approach across customers for remediation of the Agresso platform. They will be supported by EQ staff where required to update or modify integration points between Agresso and ICSIS as required. The Embridge approach runs across 4 stages.

1. Planning Phase

The planning phase will be used to mobilise the project and prepare for the upgrade. There are environment implications for two of the planning phase deliverables:

1. Complete the upgrade audit; and
2. Prepare the TEST environments

The upgrade audit has been completed as part of this Discovery exercise.

In addition, TEST environments will need to be prepared for the upgrade. This will involve:

- Provisioning an environment that has sufficient capacity to support BAU; and

- Preparing the environment with the pre-requisite tasks

  This relates to ensuring that there are appropriate Environments available to the Technical Consultants when they are made available to undertake the upgrades. These will need to have the same integration points from ISCIS to support the processing of data files both in and out.

  For BAU testing we would recommend that the Server capacities are aligned with the Production machines, SiT machines are usually to a lower specification.

  The Dev environment referred to below has already been upgraded as part of the previous ACT remediation. For this further remediation we will require a minimum of SiT1 and Pre-Production environments made available. The Production environment timing will vary in line with the overall go-live dates be that at the end of the implementation.

1. Development (DEV) - Changes will be made to the customisations source code (if required) on these environments, tracked and subject to unit tests by support analyst and developer resource. Only once successful unit testing has completed and a successful build has complied will a release be made available for deployment to further environments.

2. SiT1 -The release from the new build shall be deployed to the SIT environment initially.

3. Pre-Production (User Acceptance Testing) – The release incorporating all changes and defect resolution from Factory Acceptance Testing will be deployed to Pre-Production for User Acceptance Testing. Insolvency Staff will carry out testing on this environment to their satisfaction and sign-off. Only on successfully sign off will the release be considered ready for a LIVE deployment window.

4. Production –This is subject to successful customer sign-off of the release on Pre-Production and no priority 1 or 2 defects within the release.

2. Upgrade Phase

The TEST databases will be upgraded once the declared dependencies have been prepared.
The required report updates or enhancements outlined above will be applied to TEST once the upgrade has been completed.
EQ and Embridge Consulting use a migration based approach to application upgrade of Agresso. What this means in reality is that for each environment to be refreshed a parallel environment (consisting of relevant VM's and infrastructure configuration) is made available, with the O/S and DB level platform refresh upgrades made to it. The updated solution application (Agresso) is then deployed to these new environments and the underlying databases migrated across to the new environment. This approach provides a number of key advantages over a straight upgrade of existing environments. Namely:

- When it comes to the 'LIVE' environment, a large amount of pre-work in regards to the refresh can take place before a cutover weekend. The cutover process focuses solely on migrating the cut of LIVE data to the new servers, as opposed to carrying out the deployment and refresh from scratch.
- Roll back. A clear roll back path is provided at each stage of the tech refresh, with original environments remaining in place.
- Configuration duplication. Exact configurations and settings in terms of infrastructure and application can be observed and duplicated between environments.

3. Test Phase

Our approach to the upgrade remediation will be to upgrade and test on a 'like for like' basis unless an issue is identified as being likely to impact the upgrade, during the technical analysis phase (i.e. any defects or issues that existed before the remediation, are out of scope for explicit fixing as part of the remediation).

The TEST databases will then be ready for testing. The 2 testing cycles will take place in TEST, which are:

1. Integrated Systems Testing (IST): End to end testing run by the customer project team
2. User Acceptance Testing (UAT): Operational testing run by end users

The EQ and Embridge Consulting test approach will include the extension of the existing test strategy used within the ICSIS technical remediation project. This may include updates to existing Test Plans and Test Scripts if required. These documents will define the complete test lifecycle covering entry dependencies and exit acceptance criteria for each test phase, test progress tracking and reporting, defect tracking and resolution, and the roles and responsibilities of each party.

Test Strategy / Approach
The Test Strategy defines the approach to testing the overall solution, including test success criteria, definitions of types of defect, and including the process for managing UAT client defects identified.

The test phases enacted as part of the Agresso refresh will include:

- Unit testing (in respect of new or replacement *customisations* required),
- Integrated Systems Testing (IST), and
- User acceptance testing (UAT).

Each test phase outlines the:

- approach,
- entry/exit criteria, and
- Available test data.

Integrated Systems Testing

- Integration test results recorded

Prior to commencing of the TEST Phase of the project, Embridge will provide *TEST Management Training* to the Client, this is carried out by the Embridge Project Manager. The Embridge Project Manager will provide a testing phase tool kit to the Client Testing Manager in order to enable the Test Manager to manage the test programme effectively.

It is assumed the Client will allocate a full time Test Manager during the test cycles to ensure:

- Testing is effectively resourced by PM group team
- Test scenarios are allocated to the right business owners
- Testing is progressing to plan and managed effectively
- Testers capture issues and are logged in the right place with the right information
- Working in conjunction with the Embridge PM ensure that defects are allocated to Embridge support staff and defects fixed to allow project delivery to continue.
- Ensure the testers carry out retesting of fixed defects to allow project delivery to continue
- Coordination of regular triage meetings are held as necessary

IST involves testing the entire system for defects. The system will be tested against any available detailed design documents provided by INSS.

Test Scenarios will be prepared based on the design documents. Lifecycle scenarios and trigger events to mimic normal business operation will be created to ensure the system is fit for purpose. Test scenarios will be prepared by business testers.

The test scenarios describe the expected results, and the tester must complete the steps in the script to confirm that the required results can be produced. Each script will contain a standard set of steps, and the scenario will reference a data sheet. All test results will be captured in an excel spread sheet or Smartsheet.
The data loaded for IST is usually a subset of data (10-20%), enough to cover the scenarios included in the test plan.

IST will be managed by the Client Test Manager with support from Embridge Consultants. It is usually carried out by the project team before releasing to the end users. The testing may have limited, or no system privileges set up as the focus is on the proving of the functionality.

User Acceptance Testing

Upon completion of Integrated Systems testing and deployment the Insolvency Service will have the opportunity as part of the update programme to carry out their own functional acceptance testing inline within their own acceptance criteria before signing off the update. This signoff would be carried out before the update is deployed to the LIVE environment.

UAT will be conducted by the Insolvency Service. The User Acceptance Testing (also called Client Acceptance Test) phase concentrates on testing the system's capability to deal with the range of business scenarios it will be expected to handle; its purpose is for the Insolvency Service to be satisfied that the system has been refreshed correctly and is ready for live operation. The Supplier expects the Insolvency Service personnel to conduct UAT in order to test the complete package of software and sign-off their acceptance of it before it is implemented in the live/production environment. UAT will be based on test scripts developed by the Insolvency Service.

All defects identified during UAT which are not previously known defects, will be formally recorded, classified and audited to a satisfactory resolution using a tracking tool on a common shared repository,

utilised jointly by The Insolvency Service and EQ and provided by EQ. EQ and Embridge Consulting will rework the system and undertake all phases of the test process again before releasing any updated software to The Insolvency Service for further testing. Only when The Insolvency Service is satisfied that a defect has been resolved will it be closed in the shared database.

User Acceptance Test Entry/Exit Criteria

Entry Criteria

- Insolvency Service UAT Test Scripts
- All components installed and configured on the UAT / SIT test environment
- All critical or high severity defects hindering commencement of UAT testing must be resolved.
- All medium and low severity defects agreed for further release mutually between EQ and the Insolvency Service (Up to a maximum of 20% of all defects raised during this stage).

Exit Criteria

- UAT test scripts executed and passed
- UAT defects are logged in the Suppliers call handling repository and their status updated to prove successful retest
- All critical and high severity defects resolved and closed.
- All medium and low severity defects agreed for further release mutually between EQ and the Insolvency Service (Up to a maximum of 20% of all defects raised during this stage).
- UAT test results recorded.

3. Deploy Phase

EQ / Embridge Consulting Environments: EQ may make use of a Factory Test Environment (FAT) hosted within its infrastructure for testing purposes. All configuration of this environment would be the responsibility of EQ.

The Insolvency Service Environments: The number of Servers and specification required remains as per the detail provided above in this document. The Insolvency Service and EQ will be responsible for the following activities on the *new*, refreshed environments:-

Category	Item Name	Configuration notes
Operating System	Windows Server 2019	Default installation and configuration by Insolvency Service or their infrastructure partner
Database Management System	Microsoft SQL Server 2019	Individual database configuration to be carried out by EQ after installation of SQL 2019 by Insolvency Service.
Other Software	Unit4 ERP Release 7 update 8	Installation and configuration to be carried out by EQ and Embridge Consulting.
Client Side Software	Report Engine 9.6.3.18 Dataload 20.1.0	Installation to be carried out by Insolvency Service

Deployment Management

All deployment and release management would conform to the deployment and release stipulations within the overarching service provision and SLA. For reference this would look as follows:

Change which has a larger requirement for development, implementation or testing will be subject to a deployment methodology carried out across:

1. Development (DEV) - Changes will be made to the customisations source code (if required) on these environments, tracked and subject to unit tests by support analyst and developer resource. Only once successful unit testing has completed and a successful build has complied will a release be made available for deployment to further environments.

2. SiT1 -The release from the new build shall be deployed to the SIT environment initially.

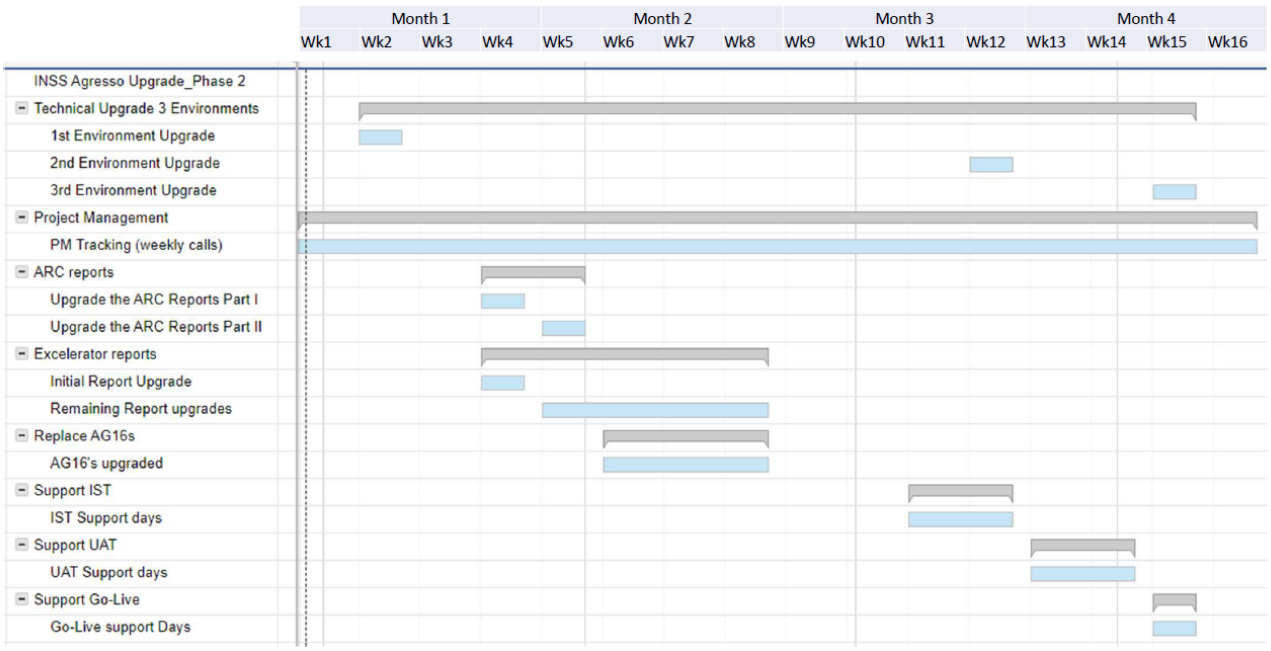
3. Pre-Production (User Acceptance Testing) – The release incorporating all changes and defect resolution from Factory Acceptance Testing will be deployed to Pre-Production for User Acceptance Testing. Insolvency Staff will carry out testing on this environment to their satisfaction and sign-off. Only on successfully sign off will the release be considered ready for a LIVE deployment window.

4. Production –This is subject to successful customer sign-off of the release on Pre-Production and no priority 1 or 2 defects within the release.

Indicative timeframe to carry out refresh

The following section incorporates an example outline plan that will be used as a baseline and adjusted accordingly to the agreed points raised above and an agreed start date.

Agresso Upgrade Phase 2 Timeline



Based on the proposed approach, work items and test requirements the indicative timeframe covers a period of 14 weeks*. It should be noted that this is based on carrying out IST and UAT test cycles on a single environment. If the INSS require IST and UAT testing to be carried out on all environments, then a corresponding period of 4 weeks per test cycle, per environment would be required.

Declared Assumptions

Ref.	Work stream	Title	Description	Owner(s)	Additional Comments
A001	Access	Embridge Staff	Access to be provided to Embridge Consultancy and sub contractor (QTC) resource to undertake technical and application upgrades	Insolvency	
A002	Install Preparation	Environments	Duplicate SIT, Pre-Prod and Production environments will be provided to the same specifications and quantity as the current SIT, Pre-Prod and production environments.	Insolvency	
A003	Interface	ICSIS Database tables	Tables used by Agresso interface stored procedures within ICSIS will remain unchanged for the duration of the refresh.	Insolvency / EQ	

Ref.	Work stream	Title	Description	Owner(s)	Additional Comments
A004	Reports	ARC Reports	Only ARC reports identified in this document as being used will be subject to being provided within Reports Xtra.	Insolvency	
A006	Database	User Defined Tables	User Defined Tables will not be subject to change or testing	Insolvency	
A007	Database	Stored Procedures	User Defined stored procedures / stored procedures formally used by WebSphere will not be subject to change	Insolvency	
A008	Initial Upgrade	Project Management & Testing Support	The proposal includes PM effort for a maximum of a 3 week period during which INSS would retain primary responsibility for defining ACT success criteria and test scenarios. Elapsed time beyond this will not have PM or Testing Support.	Insolvency	
A009	Interface	ICSIS Database tables	Tables and stored procedured used to manage the Agresso interface within ICSIS will be subject to a change freeze during remediation. Specific tables and stored procedures are as per the interface sections of this document (Pages 111 and 114)	Insolvency	

Declared Dependencies

Ref.	Work stream	Title	Description	Owner	Additional Comments
D001	Project	Access	Access to systems, and security clearance in place before project can start.	The Insolvency Service/Embridge Consulting	All activities depend on this.

Ref.	Work stream	Title	Description	Owner	Additional Comments
D002	Install Preparation	Environments	Duplicate SIT, Pre-Prod and Production environments will be provided to the same specifications and quantity as the current SIT, Pre-Prod and production environments.	Insolvency	
D003			End users with experience of the functionality, processes and their outcomes will be required to lead the UAT and IST phases of the project	Insolvency	
D004	Backup	Ledger backup	Ledgers should be backed up by the business prior to refresh on the LIVE environment	Embridge	
D005	Reports	Unused Reports	List of unused reports to be confirmed by Insolvency prior to refresh work commencing	Insolvency	
D006	AG16's	Unused AG16's	List of unused AG16's to be confirmed by Insolvency prior to refresh work commencing	Insolvency	
D007	Account Production	Functions required for account production	Funcitons required for account production. E.g. creating new short codes, account, subaccounts and associated mappings etc.	Insolvency	
D008	Browsers	Unused Browsers	List of unused browsers to be confirmed by Insolvency prior to refresh work commencing	Insolvency	
D009	Project	Staff	INSS need to have enough staff available to support the implementation of this upgrade	Insolvency	
D010	Project	Staff Experiance	INSS must inform EQ/INSS of their level of experience with ABW on a scale of 1-10? (1 is low, 10 is high)	Insolvency	
D011	Project	Original Staff	INSS must inform EQ/INCCS how many members of your original Implementation Team still work for your	Insolvency	

Ref.	Work stream	Title	Description	Owner	Additional Comments
			organisation		

Declared risks and mitigations

Ref.	Work stream	Title	Description	Owner	Impact	Likelihood	Overall Risk Rating	Mitigation
R001	ERP	Complexity	It is recognised that the application upgrade may not be simple and straight forward because INSS does not use the Agresso application like any other customer. There is a high degree of customisation and bespoke interfaces	INSS	4	2	Medium	Contingency time included within the project estimates.
R003	InfoSec	User Access	Some users utilize a combination of System and Super user roles which have unrestricted access across both data and functions.	INSS	1	5	Medium	INSS to review roles and permission access to Agresso.

Ref.	Work stream	Title	Description	Owner	Impact	Likelihood	Overall Risk Rating	Mitigation
R004	**Testing**	**UAT Testing**	Given the time that has lapsed since there was any testing on Agresso, INSS may not have good up to date test scripts to take this application through a comprehensive and thorough round of UAT testing	INSS	1	3	Medium	INSS to ring-fence staff who can effectively contribute on the generation for the UAT scripts, and add time on the proposal to have Embridge review these as required The EAS and F&C staff have detailed work instructions for how to test Agresso and how to validate that it is functioning correctly

Ref.	Work stream	Title	Description	Owner	Impact	Likelihood	Overall Risk Rating	Mitigation
R005	All	SC Clearance	Embridge staff who require SC clearance may not have 12 month minimum employment at Embridge		4	4	High	Delay in engagement due to needing to wait until suitable staff are available from other projects. EQ can provide access via its SC cleared staff.

Impact and likelihood are detailed in the Supplier's proposal: This represents the standard Supplier's criteria for defining risk and represents how risk is evaluated from the Supplier's perspective.

As fixed costs, any reference to cost increases within the proposal and within the 'Declared Risks and Mitigation' section is not applicable and is as agreed with the Supplier.

Security:

There is a requirement to have Equiniti (EQ) /Embridge/ Quickthink Cloud (QTC) staff security cleared. There will be a requirement to have 2 further Embridge staff SC cleared for the remediation and ongoing support, given previous wavier and acceptance of NPPv3 clearance.

Both the Supplier Equiniti ICS and sub-contractor Embridge staff working on this contract must be SC Cleared. The Buyer is responsible for applying for security clearance of Supplier and Embridge Consulting staff. Embridge Consulting (UK) Limited will supply personnel that currently hold NPPV3 clearance. The Supplier is responsible for providing the Buyer with the names of individuals that require security clearance at least 5 working days before their start date.

Supplier's proposal:

Version: Agresso Proposal 07.09.22 update

Agresso Proposal 07.09.22update.pdf

Out of Scope: Please note the service management proposal, pages 138 to 145 of 146 of the supplier's proposal 07.09.22 refers, is outside of the scope of this contract and relates to contract TIS0448 Equiniti Case Management Services: Provision of a Managed Service & Upgrade Services.

Schedule 2: Call-Off Contract charges

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

A fixed cost of £104,985. REDACTED

The indicative timeframe includes:

- Upgrade of the Agresso solution on a dev environment
- Testing of the Agresso solution / ACT's by the INSS
- Project Management during the above period

The indicative timeframe excludes:

- Time to have EQ/Embridge/QTC staff security cleared. There will be a requirement to have 2 further Embridge staff SC cleared for the remediation and ongoing support, given previous wavier and acceptance of NPPv3 clearance.
- Build and provision of environment
- Build and provision of test scripts and definition of success criteria.

Pricing is provided on a fixed cost basis to cover the specific core remediation and optional remediation tasks provided below. Unit testing is included within development costs. Pricing is exclusive of VAT.

As fixed costs, any reference to cost increases within the proposal and within the 'Declared Risks and Mitigation' section is not applicable and is as agreed with the Supplier.

Supplier's clarifications:

Email dated 20 September 2022

Clarification RE
Embridge and QTC I

Commercial Proposition

- Pricing is provided on a **fixed price** basis to cover the specific tasks provided below.
- Unit testing is included within development costs.
- Pricing is exclusive of VAT.

Core remediation tasks

Remediation Reference	Description	Detail	Days
de01; Page 118.	**Upgrade / Deployment** Sit/Pre-Prod LIVE Weekend Cutover Documentary Output: Installation / deployment Instructions for relevant software versions	REDACTED	REDACTED **REDACTED**
	Post Upgrade changes		
pu01; Page 107	Re-build any database views in the application that have been defined direct in the database	Included in upgrade estimates.	n/a
pu02; Page 82	Update ARC reports to Report Extra	REDACTED	REDACTED
pu03; Dependency 005	Archive unused customised reports – List of unused reports required	Included in upgrade estimates	n/a
pu04; Dependency 008	Remove any unused browsers – List of unused browsers to be agreed	Included in upgrade estimates	n/a
pu05; Page 91 Dependency 004	Remove unused AG16's – List of unused AG16s to be agreed	Included in upgrade estimates	n/a
pu06; Page 110	Remove parked VBA projects	Included in upgrade estimates	n/a

Remediation Reference	Description	Detail	Days
pu07; Page 34	Update Excelerator reports to Report Extra	REDACTED	REDACTED
pu08; Page 92	Upgrade Data Import Utilities and use flexi-field load template to replace AG16's and modify associated intellagent alerts – Technical upgrade will provide DL7 UK product	REDACTED	REDACTED
			REDACTED
	Testing		
te01; Page 122	Integration System Testing Documentary Output: Test Plan	Unit testing of Agresso pre IST	REDACTED
	Support		
su01; Page 122	UAT Support	REDACTED	REDACTED
su02; Page 124 Deployment Management	Go Live Support	n/a	REDACTED
			REDACTED
	Other / Project		
ot01; Page 135	Project Management	REDACTED	REDACTED
ot02	EQ Project Governance	Management of Embridge Consulting, escalation and project overheads.	REDACTED
			REDACTED
	TOTAL		REDACTED

Optional Remediation tasks

Remediation Reference	Description	Estimate Detail	Days	Milestone
	Post Upgrade changes			

Remediation Reference	Description	Estimate Detail	Days	Milestone
pu09; Page 26	Review of browser enquiry plus remediation as required.	REDACTED	REDACTED REDACTED	REDACTED
ot03	**Other / Project** EQ Project Governance	Management of Embridge Consulting, escalation and project overheads.	REDACTED REDACTED	REDACTED
	TOTAL		REDACTED	**REDACTED**

Milestone cost

Milestone Reference	Description	Cost
1	SIT environment completion	REDACTED
2	Pre-Production completion	REDACTED
3	Prod environment completion	REDACTED
4	Optional Production Deployment Sign Off	REDACTED
	TOTAL (Core)	REDACTED
	TOTAL (Optional)	REDACTED

Payment Milestone

Payment shall be contingent upon completion of each of the stated milestone and associated tasks above. The detailed milestone activities will be defined and agreed in the Project Plan and provided by EQ once the contract has been signed by both supplier and buyer. The acceptance criteria for MS 1, 2 3 and 4 will be defined in the project Plan and the final activity for each environment will be a sign-off milestone. The INSS Project Manager will be the sign-off authority to ensure that all activities per environment have been completed.

Additional tasks

Additional tasks outside of the fixed price work stated above, may be provided via the publicly published

Skills for the Information Age (SFIA) rate card as published on G-Cloud 12;

(https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92261/710673300926736-sfia-rate-card-2020-07-17-1227.pdf)

For reference:

	Strategy and architecture	Business change	Solution development and implementation	Service management	Procurement and management support	Client interface
1. Follow	£350	£350	£225	N/A	£350	£350
2. Assist	£425	£425	£400	N/A	£450	£450
3. Apply	£550	£550	£525	£500	£550	£550
4. Enable	£650	£650	£625	£600	£650	£650
5. Ensure or advise	£850	£850	£825	£800	£850	£850
6. Initiate or influence	£1,000	£1,000	£1,000	£1,000	£1,000	£1,000
7. Set Strategy or inspire	£1,200	£1,200	£1,200	£1,200	£1,200	£1,200

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 24months 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 theFramework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection

- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the OrderForm

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-OffContract'
2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'
2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer andSupplier as Parties under this Call-Off Contract

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

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under theterms 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 acceptancecriteria, 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 consideredto 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 hereunderif 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 14-digit ESI reference number from the summary outcome screen and promptly provide a copyto 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 theESI 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 informationsupplied by the other Party

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

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

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

6. Business continuity and disaster recovery

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

6.2 The Supplier's business continuity and disaster recovery services are part of the Servicesand 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'sown 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 ofthe Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form onreceipt 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 underthis Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Daysbefore 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 undisputedsums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts(Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if itaccepts 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 Supplieragrees 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 deathor 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 toprincipals’ 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 claimduring 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 employersliability 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 yearsafter 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 withthis 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 orthis Call-Off Contract and the Supplier will:

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

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

9.5.3 hold all insurance policies and require any broker arranging the insurance to holdany 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 legalvalidity of the insurance.

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above andthe Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

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

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

11.6.1 modify the relevant part of the Services without reducing its functionality orperformance

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

11.6.3 buy a licence to use and supply the Services which are the subject of the allegedinfringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verifyunder this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the moneypaid 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 whenProcessing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-CloudServices 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 BuyerPersonal 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 ProtectionLegislation 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 Datato 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 securesystem 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 markedBuyer 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 andthe 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 onRisk Management: https://www.cpni.gov.uk/content/adopt-risk-management-approach andProtection of Sensitive Information and Assets: https://www.cpni.gov.uk/protection-sensitive-information-and-assets

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

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

13.6.5 the security requirements of cloud services using the NCSC Cloud SecurityPrinciples 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 actionreasonably 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 foras 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 andthe Framework Agreement.

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

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

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

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

15. Open source

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

15.2 If software needs to be converted before publication as open source, the Supplier must alsoprovide 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 InformationSecurity 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 ServiceData, 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 oridentified by the Buyer when provided

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

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

16.6 Any system development by the Supplier should also comply with the government's '10Steps 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 (orequivalent) 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 theBuyer, 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 guarantorapproving 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 toprovide 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 reasonableconsidering the type of cloud Service being provided

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

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, itwill 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 effectby 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 ofthe 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 toremedy it within 15 Working Days of being notified in writing to do so

.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 materialpart 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 paywithin 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 inclause 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 orexpiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier underclauses

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

- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract whichexpressly 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 othersoftware 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 IPRsare owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer witha complete and uncorrupted version in electronic form in the formats and on mediaagreed 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 hasbeen 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 exceptif 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 asbeing '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 addresswithout any error message

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

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of serviceand 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 Termbeyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.

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

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate thatthe Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonableand 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 withits 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 andcode 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 tothe 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 ensurecontinuity 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 provideany:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer ConfidentialInformation 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 informationand 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 forreplacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

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

24. Liability

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

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

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

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

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage itcauses to the premises. It is responsible for repairing any damage to the premises or anyobjects 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 obligationsunder 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 toweaken 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 anydamage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by theHealth 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 Buyerwill 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 andany 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 noright under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. Thisdoes 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, whichthe 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 carbonfootprint.

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 willindemnify 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 toEnd 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:

2.1 the activities they perform
2.2 age
2.3 start date
2.4 place of work
2.5 notice period
2.6 redundancy payment entitlement
2.7 salary, benefits and pension entitlements

2.8 employment status
2.9 identity of employer
2.10 working arrangements
2.11 outstanding liabilities
2.12 sickness absence
2.13 copies of all relevant employment contracts and related documents
2.14 all information required under regulation 11 of TUPE or as reasonablyrequested by the Buyer

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonablypossible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

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

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

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising fromboth:

29.6.1 its failure to comply with the provisions of this clause

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

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitelyafter it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under thisclause 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 thesame 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 provideand 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 efficientoperation 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 iscalled a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to theirG-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, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement

Not 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 scopeof Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier toparticipate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreementclauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: owned by that Party before the date of this Call-Off Contract(as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract,or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the OrderForm.
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 forpurposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-OffContract.

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 theServices.
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-Offterms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplierby 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 SensitiveInformation	Information, which the Buyer has been notified about by the Supplierin writing before the Start date with full details of why the Informationis deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (butisn't limited to) any: information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including allIntellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential orwhich 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 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 onits behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to PersonalData held by the Processor under this Framework Agreement and/oractual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection ImpactAssessment (DPIA)	An assessment by the Controller of the impact of the envisagedProcessing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance andcodes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreementand in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provideunder this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.

End	Means to terminate; and Ended and Ending are construedaccordingly.

Environmental Information Regulationsor EIR	The Environmental Information Regulations 2004 together with anyguidance 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 theoutcome screen of the ESI tool.
Employment Status Indicator test tool or ESItool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
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'sperformance 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, biologicalor chemical warfare acts of government, local government or Regulatory Bodies fire, flood or disaster and any failure or shortage of power orfuel 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 inthe Supplier's (or a Subcontractor's) supply chain any event which is attributable to the wilful act, neglect or failureto 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 thatare the same as or substantially similar to the Services. This also

	includes any Subcontractor or the Supplier (or any subcontractor ofthe Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with theFramework 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 InformationAct or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codesof practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the SupplierTerms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	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, prudenceand 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 formigration), costs (for example) of implementing the services whichmay be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the requestof CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom ofInformation Act 2000.
Information security management system	The information security management system and processdeveloped by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be withinthe scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium
Intellectual PropertyRights 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 ofbeing registered in any country or jurisdiction all other rights having equivalent or similar effect in any countryor 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 ServiceCompany (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 contractedto work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine ifengagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques,methodology, and anything else in the nature of know-how relatingto the G-Cloud Services but excluding know-how already in the Supplier’s or CCS’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, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentationor otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construedaccordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or otherinformation, executable code or application software macros, whether or not its operation is immediate or delayed, and whetherthe malicious software is introduced wilfully, negligently or withoutknowledge 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 toBuyers (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 Agreementsection 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure toperform 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 theSupplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be usedby a Buyer to order G-Cloud Services.
Ordered G-CloudServices	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 assessedusing the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person 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 theperformance 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 andequipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuringconfidentiality, 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 ServicesNetwork	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations worktogether, reduce duplication and share resources.
Regulatory body orbodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate orinfluence 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 regulationsapplies.

Replacement Services	Any services which are the same as or substantially similar to any ofthe 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 athird party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Servicesfor its own account, the Buyer).
Security managementplan	The Supplier's security management plan developed by the Supplierin 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 oftheir Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on theDigital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, seehttps://www.gov.uk/service-manual/agile-delivery/spend-controls- check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provisionof G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of theSupplier 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 inrelation 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 theTerms 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 Englandand Wales.
Year	A contract year.

Schedule 7: GDPR Information

Not used