Crown Commercial Service

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM1557ix) includes:

Part A - Order Form

Digital Marketplace service ID number:	171986319631109
Call-Off Contract reference:	00264353 (previous call-off ref 00126652)
Call-Off Contract title:	Skills Manager for PD Profession
Call-Off Contract description:	IBM Kenexa Skills Manager
Start date:	21st August 2017 Additional Services commencing 15th March 2018
Expiry date:	Setup services period will expire on 20th October 2017. Licences will expire on 2nd anniversary of the first login from government department. Additional Services Expiring 31st July 2018
Call-Off Contract value:	Additional Services £38,000
Charging method:	BACS. Fixed price for setup services. Annually in advance for licences, plus additional increase in volumes paid each quarter. Additional Services are Fixed Price
Purchase order number:	TBC

This Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

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.

From: the Buyer	Cabinet Office (part of HM Gov) Buyer's main address: 1 Horse Guards Road London SW1A 2HQ

To: the Supplier	Supplier's name IBM UK Limited Supplier's address: PO Box 41 North Harbour Portsmouth PO6 3AU Company number: 741598
Together: the 'Parties'	

Principle contact details

For the Buyer:	**Title:** Capability Consultant, Infrastructure and Projects Authority **Name: REDACTED** **Email: REDACTED** **Phone: REDACTED**
For the Supplier:	Title: Government / Public Solutions Specialist Name: **REDACTED** Email: **REDACTED** Phone: **REDACTED**

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 21st August 2017 and is valid for 24 months. The Cloud Software licences will only be provisioned once the implementation services have completed.
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for disputed sums or at least **30** days from the date of written notice for Ending without cause. If ending without cause the licence fees paid for the annual charge associated with the Cloud software are non-refundable, as are any fees paid associated with implementation services.
Extension period:	This Call-Off Contract can be extended by the Buyer for two period(s) of up to 12

	months each, by giving the Supplier **1** month written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 2 - Cloud software
G-Cloud services required:	Additional Services to be provided by the Supplier under the above Lot are listed in Schedule 1 and outlined below: Services to configure IBM Skills Manager on Cloud. This Call-Off Contract outlines the Additional Services that Supplier will provide for implementation of Skills Manager for the Buyer as described below. Supplier's charges and schedule are based on performance of the activities and tasks listed in Schedule 1 of this Call-Off Contract. Deviations that arise during the project will be managed as changes through the Variation process described in clause 32 and may result in adjustments to the project scope, schedule and charges. All work for Additional Services included under this Call-Off Contract will be performed remotely by Supplier at Supplier's facilities.
Additional services:	N/A
Location:	The Services will be delivered to users via the Cloud. No specific location applies.
Quality standards:	N/A
Technical standards:	N/A
Service level agreement:	As detailed within the Supplier's Service definition document.
Onboarding:	N/A
Offboarding:	N/A
Collaboration agreement:	N/A
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £1 million The annual total liability for Buyer Data defaults will not exceed 100 % of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. The annual total liability for all other defaults will not exceed 100 % of the Charges payable by the Buyer to the 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 minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	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. Twelve (12) months after the expiry of this Call-Off Agreement period, or following termination of this Call-Off Agreement.
Buyer's responsibilities:	**Additional Services:** **1. Buyer Responsibilities** **Buyer Solution Manager** Buyer will designate a Solution Manager to communicate with Supplier and act on your behalf regarding this solution. The completion of this project depends on the full commitment and participation of Buyer's management and personnel. Buyer will perform its obligations in the Agreement and these Services without exception. Supplier's performance is predicated upon the following responsibilities being managed and fulfilled by Buyer. Delays in performance of these responsibilities may result in additional cost and/or delay of the completion of the project, and will be handled in accordance with the Change Control process. Buyer Solution Manager's responsibilities include the following: **Activity 1 - Solution Management** a. assign one project lead for the duration of the project to manage your project responsibilities under these Services, b. ensure appropriate personnel and project lead participate in all status calls, **Activity 2 - System Data Implementation** c. complete the standard Skills Manager data request form/Excel template of data; completed, clean, accurate and formatted data to Supplier. All data formatting errors will be corrected by Buyer; d. transfer your test data using Supplier's recommended secure data transfer mechanism; be responsible for Quality Assurance (QA) of your data prior to loading information into Skills Manager;

	e. review Buyer data loaded by Supplier; **Activity 3: Confirmation and Quality Assurance** f. sign-off on the production release confirming the following: (1) team data has been loaded based on team structures; (2) user data has been loaded based on team mappings; (3) job roles are loaded and mapped to skills/competencies. **Activity 4: Training** g. assign up to three persons for administrator training; h. responsible for training employees and managers in use of Skills Manager. **2. Schedule** The Services will be provided after mutual contract execution, between a start date to be determined by both parties and currently estimated to be 2 weeks after mutual contract execution and an estimated end date of 3 months after delivery of Skills Manager on the production environment, or on other dates mutually agreed to between you and Supplier. The Business Hours for the Services will be between 09:00 - 17:30 Monday to Friday UK time excluding public holidays unless otherwise determined by Supplier.
Buyer's equipment:	N/A

Supplier's information

Subcontractors or partners:	N/A

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is BACS.
Payment profile:	The payment profile for this Call-Off Contract is Fixed Price for the setup services and annually in advance for the Cloud Software.
Invoice details:	The Supplier will issue electronic invoices: upon completion of the setup services and annually in advance for the Cloud Software. Also on a quarterly basis for any increased requirements. 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 to: **REDACTED**
Invoice information required – for example purchase order, project reference:	All invoices must include a valid PO number.
Invoice frequency:	The Supplier will issue electronic invoices upon completion of the setup services and annually in advance for the Cloud Software.
Call-Off Contract value:	The total value of these Additional Services is £38,000.
Call-Off Contract charges:	**REDACTED**

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones: • A project plan will be produced at the beginning of the project detailing the tasks and deliverables associated with the implementation services
Guarantee:	N/A
Warranties, representations:	N/A
Supplemental requirements in addition to the Call-Off terms:	N/A
Alternative clauses:	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms:	N/A
Public Services Network (PSN):	N/A

1. Formation of contract

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

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

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

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557ix.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:		
Title:		
Signature:	X_____	X_____
Date:		

Schedule 1 - Services

- IBM Kenexa Skills Manager on Cloud (Service ID 171986319631109)

Additional Services:

Scope of Services

This Schedule outlines the Fixed Price Services that the Supplier will provide for implementation of Skills Manager for Buyer as described below. Supplier's charges and schedule are based on performance of the activities and tasks listed in this Schedule. In addition, the Buyer will have access to use the system for **REDACTED** employees for a 3 month pilot. Deviations that arise during the project will be managed through the Change Control process and may result in adjustments to the project scope, schedule, charges and other terms.

All work for Services included under this Schedule will be performed remotely by Supplier at Supplier's facilities.

Supplier Responsibilities

The following are Supplier's responsibilities in addition to those specified in these Services, if any.

Activity 1 - Solution Management

This activity is composed of the following tasks:

Planning & Project Management

Supplier will:

i. Assign a project manager responsible for this project and to interface with Buyer's project lead;

j. Schedule a project initiation call and provide Buyer with project kick-off preparation documents to review/complete prior to the project initiation call. During the project initiation call, Supplier will discuss the following:

   (1) Project scope/objectives;

   (2) Implementation process;

   (3) Project milestones;

   (4) Review of Standard Skills Manager data request forms to apply to Framework

k. Provide ongoing project status updates to Buyer throughout the duration of the project

Completion Criteria:

Supplier Solution Management will be complete when the Supplier Responsibilities have been performed, or when Supplier has met the criteria defined in the Completion Criteria section.

Activity outcome:

- A project plan and ongoing project status updates.

Activity 2 - System Data Implementation

Supplier will:

a. configure Skills Manager based on the following information gathered in the Standard Skills Manager data request form to apply to Framework:
    a. Organisation/Team Structure;
    b. Number of Users (linked to structure);
    c. Number of Competency Frameworks;
    d. Number of Job Roles (Categories);

b. load Buyer data as provided in the data request forms.

Completion Criteria:

System Data Implementation will be complete when the data load is complete and matches the data formatting requirements sent to the Buyer.

Activity outcome:

- ***Configure Skills Manager, based on Standard Skills Manager data request form received by Buyer***

Activity 3: System Build and Implementation

Supplier will:

l. Data Processing

Load organisation, skills and Job Role (Categories) data; map skills to Job Roles; set up administrator accounts; and obtain Customer sign-off;

m. System Set-up

Prepare server site and install Skills Manager; configure software; set up system tracking tools, and initiate system back up routines;

n. System Branding

Brand Skills Manager using the Customer's internet or intranet site as a reference (with Buyer logo and colour palette).

Completion Criteria:

System Build and Implementation will be complete when the tasks above are complete.

Activity outcome:

- ***Configure Skills Manager including: branding and standard Skill Manager Self Assessment functionality, based on Framework***

Activity 4: Confirmation and Quality Assurance

Supplier will:

a. validate that Buyer Data is loaded; and

a. conduct a walk-through of Buyer's configured site to make sure that the Buyer Data and configurations match Buyer requirements.

Completion Criteria:

Confirmation and Quality Assurance will be complete when the walkthrough is complete and the Buyer confirms the configurations have been completed according to the user requirements identified during the solution planning session(s).

Activity outcome:

- ***Signed-off user requirements by both parties that adequate quality is met***

Activity 5: Training

Supplier will:

a. provide initial webinar-based administrator training on how to use Skills Manager, including future Skills Manager releases. Administrator training is limited to three attendees assigned by Buyer; and

b. provide one softcopy of the training guides for Administrator user roles.

Completion Criteria:

This activity will be considered complete when the webinar training session is completed**.**

Activity outcome:

- ***Access to webinar training sessions and training guides***

Activity 6: Onsite Workshop & Consulting Support

Supplier will:

o. provide two 1 day workshops at either the Buyer's premises in London or Supplier's premises. The Supplier is responsible for reasonable expenses to include travel, accommodation and subsistence in relation to this activity. The Buyer must provide 5 days advanced notice to allow for scheduling and booking of travel.

p. provide up to 14hrs of additional configuration support related to activities described above.

Completion Criteria:

This activity will be considered complete when the onsite workshops have been completed**.**

Activity Outcome:

- ***Completion of 2 one day workshops and up to REDACTED hrs of additional configuration support.***

Facilities and Hours of Coverage

Supplier will

q. Perform the work remotely, except for any project-related activity which both the Supplier and the Buyer collectively determine would be best performed at the Buyer's location in order to complete its responsibilities under this Service. Under such circumstances, the Buyer would be responsible for reasonable expenses to include travel, accommodation and subsistence. The Supplier will adhere to HM Treasury Group – travel and expenses policy, or Cabinet Office travel and expenses policy.

The Business Hours for the Services will be between 09:00 - 17:30 Monday to Friday UK time, excluding UK public holidays unless otherwise determined by Supplier.

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:

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

Part B - Terms and conditions

1. Call-Off Contract start date and length

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

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)

- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.57 to 8.62 (Data protection and disclosure)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

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

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

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

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

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

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

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

5. Due diligence

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the

consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

- during this Call-Off Contract, Subcontractors hold third--party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

- a broker's verification of insurance
- receipts for the insurance premium
- evidence of payment of the latest premiums due

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

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

- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Act (DPA) or under incorporated Framework Agreement clauses 8.83 to 8.91. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

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

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, 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 publish the IPR as open source.

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

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

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- 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:

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

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

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
- other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

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

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and

following the Buyer's instructions

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

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

13. Buyer data

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

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

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

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

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

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

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
- 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, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and

accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

16.8 Additional Data Security "Security" Clauses are outlined in Schedule 7.

17. Guarantee

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

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving the notice to the Supplier specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

- Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

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

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

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

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

- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the

Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

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

19. Consequences of suspension, ending and expiry

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

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

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

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

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

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

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or

12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for

achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

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

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

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more

than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

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

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the

premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

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

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

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

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

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date in the form set out in Schedule 3.

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

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

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

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

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

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in

	the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.

Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Protection Legislation or DPA	The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Will have the same meaning as set out in the Data Protection Act 1998.
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is

	liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the

	Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557ix together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
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.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.

IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.

Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	As described in the Data Protection Act 1998 (http://www.legislation.gov.uk/ukpga/1998/29/contents)
Processing	This has the meaning given to it under the Data Protection Act 1998 as amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but

	not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-

	you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 – Data Security "Security" Clauses

1 Data Security Requirements

1.1 The Information Risk Appetite

The Buyer shall provide the Supplier with its statement of information risk appetite for the Supplier System and the Services (the "**Statement of Information Risk Appetite**"). The Supplier shall implement assurance activities to provide confidence that security control are robust and effective to be agreed with Buyer as per the principles defined within this annex**.**

1.2 Data Security Risk Acceptance

1.2.1 Security Approval to Operate (ATO) to process store and /or handle HMG data

The Supplier shall include a milestone on the Security Management plan where the Buyer provides a Security Authority to Operate before the "SERVICE" process, stores or handles HMG data. This decision will be based upon the residual risk statement which is described in the Information Risk Management Document. Any recommendation that an Authority to Operate is granted shall be approved by the Buyer. This Authority to operate shall be continually reviewed and can be revoked by the Buyer if the security risk increases to level which outside the Buyer's risk appetite.

If the Buyer unreasonably withholds its approval to the implementation of any changes proposed by the Supplier to the Information Risk Management Documentation the Supplier shall not be deemed to be in breach of this Agreement to the extent it can be shown that such breach:

has arisen as a direct result of the Buyer unreasonably withholding its approval to the implementation of such proposed changes; and

would have been avoided had the Buyer given its approval to the implementation of such proposed changes.

For the avoidance of doubt, where a change to the Information System and/or the Information Risk Management Documentation is required to remedy non-compliance with the Information Risk Management Documentation, the Baseline Security Requirements and/or any obligation in this Agreement, the Supplier shall effect such change at its own cost and expense.

If any repeat Security Assurance carried out reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default withdrawal of the Authority to Operate.

When an issue is detected which represent a risk to HMG data the Supplier shall:

propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available;

remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Information System); and

inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information System and provide initial indications of possible mitigations.

If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales defined in the Baseline Security Requirements, or as agreed with the Buyer, the Supplier must notify the Buyer immediately.

A failure to comply and manage the security risk to level which is acceptable to the Buyer shall constitute a material Default and can result in the withdrawal of the Authority to Operate. When the Authority to Operate is withdrawn the Supplier shall agree with the Buyer a data handling

management protocol.

1.3 Data Security Requirements

The Baseline Security Requirements, Annex A, defines the security requirements of the Service supplied under the Contract. The Supplier shall ensure that any subcontractor or third party service used in deliver the "SERVICE" shall be assured to an appropriate level against the Baseline Security Requirements.

The Supplier shall provide evidence to demonstrate that the "SERVICE" supplied under the Contract shall deliver the security requirements defined in the Baseline Security Requirements. This- description shall also demonstrate that the "SERVICE" incorporates the assurance best implementation practice from NCSC Security Guidance and the following specific guidance should be addressed (Annex A):

- Cloud Security Principles
- Security Design Principles
- Bulk Data Good Practice

The Supplier shall provide documentation describing how the "SERVICE" achieves the Baseline Security Requirements. This shall be agreed by the Buyer and used to inform the development of a set of agreed assurance activities. The output from these activities shall provide the Buyer that the Security Risks are being appropriately managed. This description shall include a service overview, a dataflow diagram and architectural description.

The Supplier shall outline how they propose to support the Buyer's compliance with data protection legislation throughout the life of the Contract including how it is proposed to become GDPR compliant. The Supplier shall include within their security delivery plan the resources needed to produce a Privacy Impact Assessment for the "SERVICE" where it is handling personal data.

1.4 Handling, Processing and Storage of OFFICIAL-SENSITIVE information

Where the Supplier or any third party supplier is going to handle, process and store OFFICIAL-SENSITIVE information, the Supplier shall describe how it is proposed to implement additional measures/controls to secure data of this type throughout the lifecycle of the Contract.

2. Security Assurance Activities

2.1 The Supplier shall, at its own cost and expense:

procure a CHECK IT Health Check, against a scope agreed with the Buyer, of the Information System by a NCSC approved member of the CHECK Scheme once every 12 months during the Term (each an "IT Health Check") unless additional IT Health Checks are required by Paragraph in support of implementing any "SERVICE" changes;

implement a vulnerability management process which include conducting an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Sub-Suppliers of a critical vulnerability alert from a Supplier of any software or other component of the Information System to determine whether the vulnerability affects the Information System;

conduct such other assurances as are required by:

any Vulnerability Correction Plans;

achieve ISO27001 certification;

the Information Risk Management Documentation; and

the Buyer following a Breach of Security or a significant change to the components or architecture of the Information System.

achieve Cyber Essential Scheme certification.

In relation to each Security Assurance performed the Supplier shall:

agree with the Buyer the aim and scope of the security assurance process;

promptly, following receipt/production of each Security Assurance Report, provide the Buyer with a copy of the report;

in the event that the Security Assurance Report identifies any vulnerabilities, the Supplier shall:

prepare a remedial plan for approval by the Buyer (each a "Vulnerability Correction Plan") which sets out in respect of each vulnerability identified in the Security Assurance report:

how the vulnerability will be remedied;

the date by which the vulnerability will be remedied;

the assurances which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further Security Assurance) to confirm that the vulnerability has been remedied;

in respect of each vulnerability identified in the Security Assurance report comply with the Vulnerability Correction Plan; and

conduct such further Security Assurances on the Information System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

The Security Assurances shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Service and the date, timing, content and conduct of such Security Assurances shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Assurances adversely affect the Supplier's ability to deliver the Services, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Assurances activity.

The Buyer shall be entitled to send a representative to witness the conduct of the Security Assurance activities. The Supplier shall provide the Buyer with the results of such Security Assurance processes (in a form approved

by the Buyer in advance) as soon as practicable after completion of each Security Assurance activity.

Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Agreement, the Buyer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such assurances (including penetration assurances) as it may deem necessary in relation to the Service, the Information System and/or the Supplier's compliance with the Information Risk Management Documentation. The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Security Assurances to the extent that it is reasonably practicable for it to do so taking into account the nature of the Security Assurance.

Where any Security Assurance carried out pursuant to this reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the Information System and/or the Information Risk Management Documentation (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written approval, the Supplier shall implement such changes to the Information System and/or the Information Risk Management Documentation and repeat the relevant Security Assurances in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible.

2.2 Security Delivery

2.2.1 Security Reporting

The Supplier and Buyer shall:

a) Approve/update the Security Management Plan.

b) Monitor the delivery of assurance activities

c) Manage and maintain the accuracy of the Data Security Risk Register.

d) Agree Security Assurances as being appropriate to assure delivery of security outcomes and in a manner which is consistent with the Security Assurance Framework.

e) Agree a document which presents the security residual risks and business benefit of a Service that informs the Client's decision to approve the Supplier to process, store and transit Buyer and Enabling Buyer Data associated with the Service delivery to enable presentation to the Client's Accreditation lead for approval.

f) Monitor security risk impacting upon the operation of the Services and .

g) Report of security incident in accordance with the agree Security Incident Management Process

h) Identify and agree to address any Security Requirements, out with those defined in the Baseline Security Requirements, from Buyer/Authority

i) Review/agree the Operational Security Report

2.2.2 Security Management Plan/Documentation

The Supplier shall provide as part of the produce and maintain a Security Management Plan which shall include all activities in support of security approval, documentation to be produced and security related programme milestones review post contract award. The Supplier shall maintain and update the Security Management Plan throughout the contract. The plan should include the following Data Security activities in support of the Client's security risk management:

Production/agreement of the Security Incident Management Process

Production of Information Risk Management Documentation - The purpose of this document is to enable the Supplier to complete and maintain a record throughout the lifetime of the Contract, to document the technical implementation against which the Supplier shall state compliance with the Client's Baseline Security Requirements.

Production and Maintenance of Data Security Risk Register – The purpose of this document is enable the Supplier to complete and maintain a record throughout the lifetime of the Contract, the security risks associated with the solution. The supplier shall provide a draft risk register within the tender. For each risk the supplier shall provide the following information

an assessment of the severity of the risk

description of the remediation action

target date for remediation

Security Assurance Activities – The purpose of this document is to define the security related activities which shall be undertaken to provide evidence that the "SERVICE" shall deliver the required security outcomes. This activity shall provision resource to define/agree any remediation plans and implement all remediation activity.

2.3 Operational Security Management

2.3.1 Breach of Security – General Principles

If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall notify the other in accordance with the security incident management process as set out in the Information Risk Management Documentation.

Without prejudice to the security incident management process set out in the Information Risk Management Documentation, upon becoming aware of an issue which may result in a data loss/breach the Supplier shall immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

minimise the extent of actual or potential harm caused by such Breach of Security;

remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security;

apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the Supplier, if the

mitigation adversely affects the Supplier's ability to deliver the Services, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier; and

prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure;

As soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance of the Information System and/or the Information Risk Management Documentation with the Baseline Security Requirements and/or this Framework Agreement, then such action and any required change to the Information System and/or Information Risk Management Documentation shall be at no cost to the Customer.

2.3.2 Breach of Security – IT Environment

The Supplier shall, as an enduring obligation throughout the Term, use its reasonable endeavours to prevent any Breach of Security for any reason including as a result of malicious, accidental or inadvertent behaviour. In accordance with the patching policy (which shall form part of the Information Risk Management Documentation and which shall be agreed with the Buyer), this shall include an obligation to use the latest approved version of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.

Notwithstanding section if a Breach of Security is detected in the Buyer System or the Information System, the Parties shall co-operate to reduce the effect of the Breach of Security and, particularly if the Breach of Security causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any losses and to restore services to their desired operating efficiency.

Any cost arising out of the actions of the Parties taken in compliance with the provision shall be borne by the Parties as follows:

by the Supplier where the Breach of Security originates from defeat of the Supplier's or any Sub-Supplier's security controls, the Supplier Software, the Third Party Software or the Data (whilst the Data was under the control of the Supplier);

by the Buyer if the Breach of Security originates from defeat of the Buyer's security controls or Data (whilst the Data was under the control of the Buyer); and

in all other cases each Party shall bear its own costs.

2.3.3. Vulnerabilities Management

The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information System will

be discovered which unless mitigated will present an unacceptable risk to the Data.

The severity of threat vulnerabilities for Supplier COTS Software and Third-Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Information Risk Management Documentation and using the appropriate vulnerability scoring systems including:

the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS as set out by NIST http://nvd.nist.gov/cvss.cfm); and

Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

The Supplier shall procure the application of security patches to vulnerabilities in the Information System within a maximum period from the public release of such patches as defined in the Baseline Security Requirements except where:

the Supplier can demonstrate that a vulnerability in the Information System is not exploitable within the context of the Services (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of the Services must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Services;

the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch assurance plan agreed with the Buyer; or

the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Information Risk Management Documentation.

The Supplier shall make provisions for major version upgrades of all Supplier Software and Third Party Software which are COTS Products to be kept up to date such that all Supplier Software and Third Party Software which are COTS Products are always in mainstream support throughout the Term unless otherwise agreed by the Buyer in writing.

The Supplier shall inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information System and provide initial indications of possible mitigations.

If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under the Supplier shall immediately notify the Buyer.

2.3.4 Security Threat Management

The Supplier shall:

implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, under the Cyber Information Sharing Programme or any other competent Central Government Body;

ensure that the Information System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

ensure it is knowledgeable about the trends in threat, vulnerability and exploitation that are relevant to the Information System by actively monitoring the threat landscape during the Contract Term;

pro-actively scan the Information System for vulnerable components and address discovered vulnerabilities through the processes described in the Information Risk Management Documentation;

2.3.5 Operational Security Reporting

The Supplier shall from the date specified in the Information Risk Management Approval plan and within 5 Working Days of the end of each subsequent month during the Term, provide the Buyer with a written report which details both patched and outstanding vulnerabilities in the Information System and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report.