



G-Cloud 14 Call-Off Contract Lot 2

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	12
Schedule 1: Services	33
Schedule 2: Call-Off Contract charges	34
Schedule 3: Collaboration agreement	35
Schedule 4: Alternative clause	48
Schedule 5: Guarantee	52
Schedule 6: Glossary and interpretations	60
Schedule 7: UK GDPR Information	76
Annex 1: Processing Personal Data	76
Annex 2: Joint Controller Agreement	80
Schedule 8: Corporate Resolution Planning	88
Schedule 9: Variation Form	110

Part A: Order Form

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

Platform service ID number	814682357597846
Call-Off Contract reference	C331325
Call-Off Contract title	Cyber Risk Insights Licence - Platinum
Call-Off Contract description	Licensing of KPMG Cyber Risk Insights, risk quantification software.
Start date	The date of the last signature on this Order Form
Expiry date	31st March 2027
Call-Off Contract value	<p>The initial contract term value is £192,593 (ex VAT) for 26 months.</p> <p>The total value of the contract is £192,593 ex VAT</p> <p>Value of optional extension for up to 10 months: £74,074 ex VAT</p>
Charging method	Invoice
Purchase order number	To be Provided

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

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

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

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

From the Buyer	NHS England 7 - 8 Wellington Place Leeds West Yorkshire LS1 4AP
To the Supplier	KPMG LLP +44 (0) 20 7311 1000 15 Canada Square London England E14 5GL United Kingdom Company number: OC301540

Together the 'Parties'

Principal contact details

For the Buyer:

Title: Cyber Improvement Programme Design Lead

Name: [REDACTED]

Email: [REDACTED]@nhs.net

Phone: [REDACTED]

For the Supplier:

Title: Director

Name: [REDACTED]

Email: [REDACTED][@kpmg.co.uk](mailto:[REDACTED]@kpmg.co.uk)

Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on the date of the last signature on this Order Form and is valid for 26 months .
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).

<p>Extension period</p>	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 10 months, by giving the Supplier 4 weeks written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p> <p>The Parties acknowledge and agree that the Call-Off Contract shall not automatically renew.</p>
--------------------------------	--

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.

<p>G-Cloud Lot</p>	<p>This Call-Off Contract is for the provision of Services Under:</p> <p>Lot 2: Cloud software</p>
<p>G-Cloud Services required</p>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined below:</p> <ul style="list-style-type: none"> • Licensed access to KPMG Cyber Risk Insights, risk quantification software • Unlimited users (fair usage of up to a maximum of 1000 concurrent users – being those users using the CRI Service at the same time) • Platinum Tier (see the 'Platinum Tier' Services as described in Schedule 2 (<i>Call-Off Contract charges</i>)) <p>The Services do not include any implementation or advisory services (except the onboarding, offboarding, support and other services expressly set out in this Order Form) which is</p>

	subject to a separate engagement between the Parties.
Additional Services	N/A
Location	Data stored in Microsoft Azure's (the Supplier's cloud hosting service provider) data centres in the UK.
Quality Standards	<p>In addition to the standards required in Part B of this Call-Off Contract, the quality standards required for this Call-Off Contract are as follows. The product shall:</p> <ul style="list-style-type: none"> ● Provide functionality as described in the service definition document published on the Gov UK Digital Marketplace in the form set out in Annex B to this Order Form. ● Be free from known critical defects at the time of release. ● Include accurate versioning and change logs for transparency. ● Have an intuitive user interface that aligns with modern design principles. ● Include clear user instructions and contextual help. ● Ensure data accuracy through built-in validation mechanisms. ● Use resource efficient design to minimise system impact.
Technical Standards:	<p>In addition to the standards required in Part B of this Call-Off Contract, the technical standards used as a requirement for this Call-Off Contract are as follows. The product shall:</p> <ul style="list-style-type: none"> ● Be compatible with major operating systems and browsers. Currently, the product is supported by current versions of Microsoft Edge, Google Chrome and Safari. ● Use modern, scalable architecture for optimal performance and maintenance. ● Follow industry-standard software development

	<p>methodologies (Agile and DevOps) and coding best practices, including proper version control.</p> <ul style="list-style-type: none"> • Include comprehensive testing protocols covering functionality, security and performance. • Support software updates with minimal downtime. • All Services to comply with the Data Security and Protection Toolkit and Cyber Essentials Plus
<p>Service level agreement:</p>	<p>The following sections provide details on service availability, monitoring and related information.</p> <p>1 Service Availability Availability specifics relating to the Service (specifically here the CRI software) provided by KPMG (“we” or “us”) are as follows:</p> <p>1. Web based services As a software-as-a-service (SaaS), CRI’s Service availability is subject to the factors specified below.</p> <p>We will make CRI’s web-based services available for a minimum of 99% of time within each calendar month. “Available” means that the Service is operating, all basic functions are accessible, and the Service is functioning in accordance with the Service description at Annex B. If the Availability of the Service falls below 95% of the time in any calendar month, this shall be treated as the Supplier’s Material Breach as per clause 18.5 of Part B.</p> <p>Scheduled Maintenance, Force Majeure events and Unscheduled Emergency Maintenance will be excluded from the downtime. “Scheduled Maintenance” means any work notified to the customer (as set out in section 2 below) to be carried out that may cause the Services to be temporarily suspended or disrupted. The Supplier shall take all reasonable measures to ensure that Scheduled Maintenance is carried out in non-Working Hours and that there is no more than 7 hours of Scheduled Maintenance in any one month. Where Scheduled Maintenance is required in Working Hours, notice will be provided (as set out in section 2 below).</p> <p>“Unscheduled Emergency Maintenance” is maintenance which is urgently required to address a serious security issue or serious functional issue in the CRI Service (excluding issued caused by Supplier or its Subcontractors) and will be performed as needed, with the Supplier restoring the Service as soon as possible (using all reasonable endeavours to do so within the resolution targets at 1.5 below), and CRI will make all reasonable efforts to notify customers in advance.</p>

	<p>2. Email support</p> <p>Email support is provided during Working Hours. “Working Hours” means 9am to 5pm UK time on Business Days. “Business Days” means any day other than Saturday or Sunday or bank or public holidays in England.</p> <p>Emails received outside of Working Hours will be collected, however no action can be guaranteed until commencement of Working Hours on the next Business Day.</p> <p>Contact details for support are as follows: crisupport@kpmg.co.uk.</p> <p>3. Support requests</p> <p>Support requests will be dealt with on a priority basis as reasonably determined by us. Priority is determined through a combination of impact and urgency, as described below. Support requests do not include new feature requests.</p> <p>4. Priority definitions</p> <p>Each support request shall be assigned a priority on receipt by us:</p> <p>Priority 1:</p> <ul style="list-style-type: none">• The issue or failure is causing immediate and significant impact on major business functions for the users pursuant to this Agreement. There is no possible workaround. <p>Priority 2:</p> <ul style="list-style-type: none">• The issue or failure is causing immediate and significant impact on major business functions for the users pursuant to this Agreement, but there is a workaround available; or• the issue will imminently cause significant impact on major business functions for the users pursuant to this Agreement and there is no possible workaround; or• the issue is causing critical and significant impact on non-core business functions of the users pursuant to this Agreement and there is no possible workaround. <p>Priority 3:</p> <ul style="list-style-type: none">• The issue or failure is causing an impact on non-core business functions of the users pursuant to this Agreement, and a workaround is available. <p>Priority 4:</p> <ul style="list-style-type: none">• The issue or failure has limited impact, or the impact is minimal, and a workaround will be provided in the next calendar month. <p>1.5 Target response and resolution targets</p>
--	---

We will respond to, and to satisfactorily resolve, 90% of issues (100% of Priority 1 issues) submitted to the mailbox within the targeted time, as specified below.

Priority	Target response time – non-automated confirmation by email that the issue has been received and assigned priority	Target resolution time
1	8 Working Hours	24 Working Hours
2	8 Working Hours	48 Working Hours
3	2 Business Days	10 Business Days
4	2 Business Days	20 Business Days

In the event that the Supplier does not meet the response and resolution times for a Priority 2, 3 or 4 issue (without prejudice to the Buyer's other rights and remedies), the Priority of that issue shall be escalated to the level above. For example, a P4 will become a P3 (and it shall then become a P2 if the P3 response or resolution times are not met, and so on).

Target response and resolution times reference above will be measured from whichever is the latter of:

- When we receive a support request and such information is sufficient in order for us to give the issue a priority
- If there is ambiguity of whether the fault lies with CRI's or Buyer's (or its users') browser, single sign-on system, or internet connection, from when CRI's engineers have confirmed (acting promptly in accordance with the response timescales above) that the fault is with CRI.

1.6 Exceptions

When a support request requires information or support from the external vendors (Microsoft Azure or the processors agreed in Schedule 7) which is outside of the Supplier's reasonable control (or more information from the Buyer), we may take longer than the above periods to resolve such issues. Such additional time will not be counted as part of the target resolution times provided that the Supplier shall use all reasonable endeavours to resolve the issue promptly and shall keep the Buyer informed regularly (in line with the response times above) of its progress towards a resolution and reasonable expected timescales.

2. Scheduled maintenance

We shall provide the following minimum levels of notice in respect of Scheduled Maintenance:

	<table border="1" data-bbox="639 203 1468 414"> <thead> <tr> <th data-bbox="639 203 1050 309">Maximum expected outage period during a Business Day's Working Hours</th> <th data-bbox="1050 203 1468 309">Minimum notice</th> </tr> </thead> <tbody> <tr> <td data-bbox="639 309 1050 342">30 minutes</td> <td data-bbox="1050 309 1468 342">24 hours</td> </tr> <tr> <td data-bbox="639 342 1050 376">1 hour</td> <td data-bbox="1050 342 1468 376">5 business days</td> </tr> <tr> <td data-bbox="639 376 1050 414">More than 1 hour</td> <td data-bbox="1050 376 1468 414">10 business days</td> </tr> </tbody> </table> <p data-bbox="639 450 1468 584">Where there is no expected outage, or adverse impact on the Buyers' or users' use of the Service (or the functionality of the Service), for software updates or release of new functionality, there is no requirement to provide notice.</p>	Maximum expected outage period during a Business Day's Working Hours	Minimum notice	30 minutes	24 hours	1 hour	5 business days	More than 1 hour	10 business days
Maximum expected outage period during a Business Day's Working Hours	Minimum notice								
30 minutes	24 hours								
1 hour	5 business days								
More than 1 hour	10 business days								
<p data-bbox="202 703 371 741">Onboarding</p>	<p data-bbox="639 703 1410 741">The onboarding plan for this Call-Off Contract is as follows:</p> <ul data-bbox="687 770 1425 1995" style="list-style-type: none"> <li data-bbox="687 770 1425 804">● Set up your dedicated workspace within the product. <li data-bbox="687 835 1425 1328">● Create user accounts with appropriate roles and permissions (as agreed with you) for initial Buyer including setting up the Buyer as a workspace owner (and the Buyer's workspace owner users required by the Buyer) within 5 working days of the start date of this Call-Off Contract ("User Set-Up Timescales"). The Supplier shall ensure that the Buyer has the tools to enable the Buyer to set up additional workspace owners and all other users itself (including any users of Eligible Public Health Bodies which are accepted in accordance with the process set out in the Supplemental requirements section of this Order Form). <li data-bbox="687 1359 1425 1469">● Send welcome emails to activate accounts and explain key platform details within the User Set-Up Timescales. <li data-bbox="687 1500 1425 1653">● Hold an initial session to discuss your planned use of the product to ensure requirements are understood by the Parties and introduce you to your Customer Success Manager. <li data-bbox="687 1684 1425 1794">● Led by your Customer Success Manager, hold a joint success planning session to enable a common understanding of what success looks like. <li data-bbox="687 1825 1425 1897">● Agree a complementary plan of action alongside relevant advisory work being completed. <li data-bbox="687 1928 1425 1995">● Hold up to three training sessions with initial users, provide a walkthrough of the product's key features 								

	<p>and interface.</p> <ul style="list-style-type: none"> • Provide access to self-service resources through our knowledge base. • Provide a clear contact point for technical support. • Schedule regular (at least weekly) progress check-ins during the onboarding.
--	--

<p>Offboarding</p>	<p>In addition to the exit plan requirements set out in Clause 21 of Part B of this Call-Off Contract, the offboarding plan for this Call-Off Contract is as follows:</p> <ul style="list-style-type: none"> • provide a single point of contact to coordinate the Supplier’s activities and liaise with the Buyer to ensure that all reasonable activities to support the orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier. • Disable user accounts and revoke system access. • Notify users of account termination with key dates. • Clause 19.5 of Part B shall apply in respect of the return and destruction of Buyer Data (and other materials as set out in Clause 19.5) at the expiry or termination of the Call-Off Contract) subject to the following: <ul style="list-style-type: none"> ○ the supplier may retain general electronic back-ups for up to 180 days following expiry or termination of the Call-Off Contract; ○ the Supplier may retain Buyer Data contained in its systems logs in accordance with its retention policies provided that such data shall be secured and processed in accordance with its obligations under the Call-Off Contract and applicable laws; ○ unless instructed otherwise by the Buyer in advance, the Supplier shall provide the Buyer with all capability effectiveness input data in CSV format within 15 Working Days of the expiry or termination of the Call-Off Contract; and
---------------------------	---

	<ul style="list-style-type: none"> ○ the Supplier shall ensure that the Buyer has access which enables the Buyer to obtain its own copies of the Project Specific IPRs from the Service. <p>Nothing in the above shall limit the Supplier's right to retain Buyer Data where required by Law.</p> <p>In addition, at the expiry or termination of this Call-Off Contract the Supplier will:</p> <ul style="list-style-type: none"> ● Deactivate your workspace. ● Confirm settlement of all contractual obligations. ● Conduct an exit survey to gather user feedback.
<p>Collaboration agreement</p>	<p>Not Applicable.</p>
<p>Limit on Parties' liability</p>	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £[REDACTED] or [REDACTED]% the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>Subject to incorporated Framework Agreement clause 28.2, the annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed £[REDACTED] or [REDACTED]% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the greater of £[REDACTED] or [REDACTED]% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>

<p>Buyer's responsibilities</p>	<p>The Buyer is responsible for:</p> <ul style="list-style-type: none"> ● Using the software in compliance with all applicable laws and regulations. ● Ensure that users adhere to the acceptable use policy agreed between the Parties. In the event of any breach by an Eligible Public Health Body (or any of its users) of the acceptable use policy agreed by the Parties (AUP) or this Call-Off Contract, the Supplier's primary remedy and mitigation shall be to terminate or suspend the relevant user's (or users') access to the Service in accordance with the AUP. ● Provide accurate and timely information reasonably required for setup and maintenance. ● Maintain responsibility for data accuracy of Buyer Data as provided or modified by the Buyer or its users. ● Implement internal security practices to protect user credentials. ● Maintain a standard modern internet browser. ● Report issues promptly with reasonable details for troubleshooting. ● Reasonably cooperate with technical support to resolve issues efficiently.
<p>Buyer's equipment</p>	<p>The Buyer's equipment to be used with this Call-Off Contract includes Buyer's computers (or the Authorized Users' computers, as applicable).</p> <p>Reason To access the product.</p>

Supplier's information

<p>Subcontractors or partners</p>	<p>Not Applicable</p>
--	-----------------------

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 Bank Transfer from Invoice
Payment profile	The payment profile for this Call-Off Contract is payment of Licence fees for 26 months in advance.
Invoice details	<p>The Supplier will issue electronic invoices within 30 days of the Order Form commencing and receipt of a Purchase Order. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice which includes a valid Purchase Order Number. The Buyer may, without prejudice to any other rights and remedies under this Call-Off Contract withhold or reduce payments in the event of unsatisfactory performance.</p> <p>All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Buyer shall, following the Receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.</p>
Who and where to send invoices to	<p>Invoices should clearly quote the purchase order number, be addressed to NHS England, T56 Payable A125, PO Box 312, LEEDS LS11 1HP and be sent as a PDF attachment by email to the following email address; sbs.apinvoicing@nhs.net (one invoice per PDF) and emails must not exceed 10Mb and quote, 'T56 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.</p> <p>Any queries regarding outstanding payments should be directed to NHS England (NHS Digital)'s Accounts Payable section by email at financialaccounts@nhs.net</p>
Invoice information required	The Buyer shall issue a Purchase Order to the Supplier in respect of any Services to be supplied to the Buyer under this Call-Off Contract. The Supplier shall comply with the terms of such Purchase Order as a term of this Call-Off Contract. For the avoidance of doubt, any actions or work undertaken by the Supplier under this Call-Off Contract prior to

	<p>the receipt of a Purchase Order covering the relevant Services shall be undertaken at the Supplier's risk and expense and the Supplier shall only be entitled to invoice for Services covered by a valid Purchase Order.</p> <p>The Supplier must be in Receipt of a valid Purchase Order Number before submitting an invoice. All invoices should be sent, quoting that number to the address given on the Purchase Order. To avoid delay in payment it is important that the invoice is compliant and that it includes an item number (if applicable) and the details (name and telephone number) of the Buyer contact. Non-compliant invoices will be sent back to the Supplier, which may lead to a delay in payment.</p>
Invoice frequency	Invoice will be sent to the Buyer in accordance with the above payment profile.
Call-Off Contract value	Has the meaning given in Part A, above
Call-Off Contract charges	<p>The breakdown of the Charges is as set out in Order Form Schedule 2 (Call-Off Contract charges).</p> <p>Any expenses must be agreed by the Buyer in writing prior to such costs being incurred and will only be payable in accordance with the Buyer's expenses policy.</p>

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> • Your workspace will be provisioned within 2 business days after execution of this Order Form. • Access will be provisioned for initial users within 1 business day of confirmation of initial users by the Buyer.
-----------------------------------	---

	<ul style="list-style-type: none"> Onboarding and offboarding will include the details from the relevant sections above.
Guarantee	Not Applicable
Warranties, representations	<p>In addition to the incorporated Framework Agreement clause 2.3, the Supplier will comply with the warranties and representations set out in the Buyer specific amendments to/refinements of the Call-Off Contract terms.</p> <p>The Supplier warrants that the Services will be provided in conformity with and meet all requirements and standards set out in this Call-Off Contract.</p>
Supplemental requirements in addition to the Call-Off terms	<p>(The Supplier Terms, available on Gov.UK Digital Marketplace here: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/93303/814682357597846-terms-and-conditions-2024-05-01-1131.pdf supplement and are additional to the Call-Off Contract Terms and Conditions; the applicability and order of priority of such Supplier Terms being as set out in clause 8.3.4 of the Framework Agreement).</p> <p>The following requirements shall take priority above all terms, conditions and specifications set out in this Call-Off Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that the software licences meet and conform with the following requirements:</p> <ol style="list-style-type: none"> Subject to supplemental clauses 2 and 3 below, Authorised Users (as defined in the Supplier Terms) of the Services may also include employees, officers, contractors or other workers from any “Eligible Public Health Body (or Bodies as the case may be)” which shall mean: <ol style="list-style-type: none"> NHS England and its successor organisations; NHS Trusts, NHS Foundation Trusts, and any other healthcare provider organisations forming part of the NHS structure in England;

	<p>c) Any publicly funded health or social care organisation established or authorised by statute, regulation, or government policy to operate within the NHS or provide public health services in England; and</p> <p>d) Any other entity that assumes the functions, roles, or responsibilities of the above organisations as a result of reorganisation, merger, name change, or other structural changes within the NHS or public health sector.</p> <p>This definition is intended to include all relevant organisations operating within the public health or social care framework of England, as may be updated or modified from time to time. Such bodies include the bodies listed in Annex A to this Call-Off Contract and any other bodies notified by the Buyer from time to time.</p> <p>2. Access to the Services to any Eligible Public Health Body is subject to completion of the below notification and onboarding process.</p> <p>3. Notification and Onboarding Process for Eligible Public Health Bodies:</p> <p>i. Notification Requirement: Prior to granting access to the Service to any proposed Eligible Public Health Body, Buyer shall provide Supplier with written notification including the following details of the proposed Eligible Public Health Body (or such other details as Supplier may reasonably require):</p> <ul style="list-style-type: none">a. Full legal entity name;b. Registration number (if applicable); andc. Registered address. <p>ii. Method of Notification: The information set out above shall be submitted by email to crinhsonboarding@kpmg.co.uk.</p> <p>iii. Onboarding Checks: Upon receipt of the notification, Supplier shall conduct the following procedures to evaluate prospective clients and engagements and shall confirm in writing within 20 Working Days of the Buyer's notice in 3(i) above either: (a) whether or not the Eligible Public Health Body is able to be onboarded; or (b) if the Supplier (acting reasonably and in good faith) requires more time to conduct the checks due to the complexity and extent of the searches required (in which event the Supplier shall notify Buyer of a reasonable timescale in which it shall complete its checks).</p> <ul style="list-style-type: none">- The Supplier's checks shall involve checking compliance with laws, rules, regulations or professional standards, and for circumstances that would cause the relationship between the parties to violate such law, rule, regulation or professional standard ("Rules") or would prejudice Supplier's ability
--	---

to comply with applicable auditor independence requirements .

The proposed Eligible Public Health Body shall not be granted access to the Service until the Supplier has completed the above checks and Supplier (acting reasonably) has confirmed, in writing, that access may be granted (and Eligible Public Health Bodies shall only be rejected if either: (a) they fail the above specified checks; or (b) there are other unforeseeable or extenuating circumstances outside of the Supplier's control which require the Supplier, acting reasonably, to reject such Eligible Public Health Body, and in both cases the Supplier shall (to the extent permitted under the Rules), on Buyer's request provide written reasons for rejecting any Eligible Public Health Body).

- iv. Buyer Timing and Compliance: Buyer shall ensure that the required notification is made in a timely manner to allow the Supplier sufficient time to complete its checks. Any failure by Buyer to comply with this process may result in a delay of access to the Service by the Eligible Public Health Body.

Indemnity

Subject to the liability cap set out in clause 24.1 of Part B of this Call-Off Contract, to the fullest extent permitted by law, Buyer agrees to indemnify Supplier against all Loss arising from any action, proceeding or claim brought or threatened against the Supplier by an Eligible Public Health Body, where such action, proceeding, or claim arises out of, results from, or is connected with: a) the misuse of the Service by an Eligible Public Health Body to whom access has been provided not in accordance with the terms of this Call-Off Contract (or any Acceptable Use Policy (AUP) relevant to the Services which is agreed by the Parties); or b) any failure by the Buyer to comply with the these supplemental clauses set out here in; or c) any act, omission, or misrepresentation by Buyer in relation to the Services.

The Buyer hereby agrees that no Eligible Public Health Body except the Buyer (NHS England) shall bring a claim against the Supplier in respect of loss or damage suffered by the Buyer or an Eligible Public Health Body in connection with this Call-Off Contract or the Services. The Parties agree that that Buyer shall be entitled to bring a claim against the Supplier for all Losses suffered by any Eligible Public Health Body as a result of the

	<p>Services (or the acts or omissions of the Supplier or Supplier Staff) as if the Eligible Public Health Body's Losses were the direct Losses of the Buyer. To the fullest extent permitted by law, the Supplier's total aggregate liability arising out of or in connection with this Call-Off Contract or the Services shall be limited in accordance with the "limit on parties liability" section above and Clause 24.2 of Part B, which shall apply in aggregate for all claims, including but not limited to those brought by the Buyer and/or any Eligible Public Health Bodies granted access to the Service.</p> <p>Nothing in these Supplemental requirements affects the Parties' duty to mitigate their loss.</p> <p>4. Any software licenced to the Buyer on a named user basis shall permit the transfer from one user of the Buyer or an Eligible Public Health Body to another user of the Buyer or of that Eligible Public Health Body, free of charge provided that the Supplier is notified of the same (including without limitation to a named user who is a contractor and/or Subcontractor of the Buyer or Eligible Public Health Body who requires access for the purpose set out in this Call-Off Contract).</p> <p>5. The Supplier shall notify the Buyer in advance if any software or service permits the Supplier or any third-party remote access to the software or systems of the Buyer.</p>		
<p>Alternative clauses</p>	<p>Not Applicable</p>		
<p>Buyer specific amendments to/refinements of the Call-Off Contract terms</p>	<table border="1"> <tr> <td data-bbox="549 1621 810 1957"> <p>Buyer Data</p> </td> <td data-bbox="810 1621 1327 1957"> <p>all data supplied by the Buyer (or an Eligible Public Health Body, or any of their users) to the Supplier (including Personal Data and Service Data that is owned, provided or managed by the Buyer or an Eligible Public Health Body or their users);</p> </td> </tr> </table>	<p>Buyer Data</p>	<p>all data supplied by the Buyer (or an Eligible Public Health Body, or any of their users) to the Supplier (including Personal Data and Service Data that is owned, provided or managed by the Buyer or an Eligible Public Health Body or their users);</p>
<p>Buyer Data</p>	<p>all data supplied by the Buyer (or an Eligible Public Health Body, or any of their users) to the Supplier (including Personal Data and Service Data that is owned, provided or managed by the Buyer or an Eligible Public Health Body or their users);</p>		

	<p>Buyer Personal Data</p>	<p>The Personal Data supplied by the Buyer (or an Eligible Public Health Body, or any of their users) to the Supplier for purposes of, or in connection with, this Call-Off Contract.</p>
	<p>Central Government Body</p>	<p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none"> a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; and d) Executive Agency;
	<p>Cyber Security Requirements</p>	<p>means:</p> <ul style="list-style-type: none"> a) compliance with the DSP Toolkit or any replacement of the same; <p>and</p> <ul style="list-style-type: none"> c) any other cyber security requirements relating to the Services notified to the Supplier by the Buyer from time to time;
	<p>DSP Toolkit</p>	<p>means the data security and protection toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards and supports key requirements of the GDPR, which can be accessed</p>

		<p>from https://www.dsptoolkit.nhs.uk/, as may be amended or replaced by the Buyer or the Department of Health and Social Care from time to time;</p>
<p>Project Specific IPRs</p>	<p>means 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 all reports, results and other outputs generated by the Supplier's CRI tool but not including the Supplier's Background IPRs or Third Party IPRs;</p>	
<p>Purchase Order</p>	<p>means the Buyer's unique number relating to the supply of the Services;</p>	
<p>Receipt</p>	<p>means the physical or electronic arrival of the invoice at the address specified above at 'Call-Off Contract charges and payment' under the heading "Who and where to send invoices to" or at any other address given by the Buyer to the Supplier for the submission of invoices from time to time;</p>	
<p>Third Party IPRs</p>	<p>means any intellectual property rights owned by a third party, which are licensed by the Supplier for the purposes of providing the Services;</p>	
<p>1) New Clauses 11.10 to 11.14 inclusive, shall be added to</p>		

	<p style="text-align: center;">Clause 11 of the Call-Off terms, as follows:</p> <p>11.10 All Project Specific IPRs shall vest in the Buyer absolutely, and the Supplier hereby assigns to the Buyer, absolutely with full title guarantee (and free from all third party rights), any and all of its right, title and interest in and to all the existing and future Project Specific IPRs, to the fullest extent permitted by law.</p> <p>11.11 The Supplier grants to the Buyer (and to Eligible Public Health Bodies who pass the onboarding checks set out in the 'Onboarding' section above) a non-exclusive, transferable (in accordance with clause 11.14 below) perpetual, irrevocable, royalty-free licence to use any Supplier Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities and to the extent required to enjoy the full benefit of ownership of the Project Specific IPRs.</p> <p>11.12 The Buyer shall have the right to grant to any person a sub-licence of any licence granted pursuant to Clauses 11.11.</p> <p>11.13 Each Party undertakes that it shall promptly execute all documents, make all applications, give all assistance and do or procure the doing of all acts and things as may be necessary or desirable to give full effect to the assignment of the Project Specific IPRs described in Clause 11.10 in, and to register ownership of the Project Specific IPRs in, the name of the Buyer (to the extent that registration of rights is available) and/or to give full effect to the licences granted under this Clause 11.</p> <p>11.14 The licence granted by the Supplier under Clause 11.4 shall be transferable to other Central Government Bodies.</p> <p>2) The Supplier acknowledges and agrees that there will be no unavoidable Loss by the Supplier under clause 18.3 of Part B.</p> <p>4A IR35 -not applicable</p> <p>4B Security of Supplier Staff</p> <p>4B.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard:</p>
--	--

	<p>https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as may be amended or replaced by the Government from time to time.</p> <p>4B.2 The Supplier shall agree on a case by case basis which Supplier Staff roles require specific government National Security Vetting clearances (such as 'SC' and 'BPSS') including system administrators with privileged access to IT systems which store or process Buyer Data.</p> <p>4B.3 The Supplier shall prevent Supplier Staff who have not yet received or are unable to obtain the security clearances required by this clause from accessing systems which store, process, or are used to manage Buyer Data, or from accessing Buyer premises, except where agreed with the Buyer in writing.</p> <p>4B.4 All Supplier Staff that have the ability to access Buyer Data or systems holding Buyer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.</p> <p>4B.5 Where Supplier Staff are granted the ability to access Buyer Data or systems holding Buyer Data, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need such access or leave the organisation, their access rights shall be revoked within one (1) Working Day.</p> <p>3) A new Clause 16.8 shall be added as follows:</p> <p>16.8 The Supplier warrants and represents that it has complied with and throughout the Call Off Contract Period will continue to comply with the Cyber Security Requirements.</p> <p>4) Clauses 12.1 and 12.3 of the Call-Off terms and conditions shall be deleted in their entirety and replaced with the following new Clauses 12.1 and 12.3:</p> <p>12.1 These Clauses 12.1 and 12.3 shall apply only where and to the extent the Supplier processes Buyer Personal Data as a 'processor' on behalf of the Buyer. The Supplier must:</p> <ul style="list-style-type: none">• comply with the Buyer's written instructions and this Call-Off Contract when Processing any Buyer Data, including but not limited to Buyer Personal Data;
--	---

	<ul style="list-style-type: none"> • only Process the Buyer Data, including but not limited to 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 any Buyer Data, including but not limited to Buyer Personal Data act in compliance with Supplier's security processes. <p>12.3 The Supplier must get prior written consent from the Buyer to transfer any Buyer Data, including but not limited to Buyer Personal Data to any other person including any Subcontractors) for the provision of the Services.</p> <p>12.7 Neither Party shall do nor omit to do anything that will put the other Party in breach of the Data Protection Legislation.</p> <p>5) Clause 13.2 of Part B shall be deleted and replaced as follows:</p> <p>The Supplier will only use the Buyer Data (including but not limited to Buyer Personal Data, whether or not the Buyer is the Controller) and Project Specific IPR during the Term, and only to the extent necessary to fulfil its obligation to provide the Service under this Call-Off Contract or as required by Law or any Regulatory Body. The Supplier will not (except in accordance with the 'Offshore Working' part of this Order Form) transfer any Buyer Data which is Personal Data outside of the UK other than to the processors listed under Schedule 7 in accordance with section 13) below (Data Transfers).</p> <p>6) A new clause 7.2A shall be added to the Call-Off terms and conditions as follows:</p> <p>7.2A Electronic Invoicing</p> <p>7.2A.1 The Buyer shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.</p> <p>7.2A.2 For the purposes of clause 7.2A.1, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU)</p>
--	---

	<p>2017/1870.</p> <p>7) New Clause 33.2 shall be added as follows:</p> <p>Data Protection Impact Assessment Delivery and Assistance</p> <p>33.2 Without limitation to the obligations as set out in Schedule 7 (UK GDPR Information), the Call-Off Contract and the Order Form, the Supplier shall participate and provide reasonable co-operation for the completion of any Data Protection Impact Assessments conducted by the Buyer relating to the Services and the deliverables. Such participation and co-operation shall include updating the Data Protection Impact Assessment at each material change of the deliverable(s) (including but not limited to each release of new software) and following any Variation.</p> <p>8) A new Clause 34 shall be added as follows:</p> <p>34 Assignment and Novation</p> <p>The Buyer may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Call-Off Contract and/or any associated licences free of charge (save for the payment of any Charges) to the Department of Health and Social Care (or, on notice to the Supplier, to any entity which is a successor body to the Buyer (or its successors), or which otherwise performs any or all of the functions of the Buyer (or its successors), except that, where the Supplier is prohibited at law or by its regulatory or professional obligations from contracting with or providing the Service to such successor entity, the Supplier shall be entitled to object to such assignment or transfer). Supplier shall, at the Buyer's request, enter into an agreement in such form as the Buyer shall reasonably specify in order to enable the Buyer to exercise its rights pursuant to this clause 34 (Assignment and Novation).</p> <p>9) A new Clause 35 shall be added as follows:</p> <p>35 Supplier shall ensure that each material Subcontract shall include:</p> <p>35.1 a right under the Contracts (Rights of Third Parties) Act 1999 for the Buyer to enforce any provisions under the material Subcontract which confer a benefit upon the Buyer;</p>
--	--

	<p>35.2 a provision enabling the Buyer to enforce the material Subcontract as if it were the Supplier; and</p> <p>35.3 obligations no less onerous on the Subcontractor than those imposed on the Supplier under this Call-Off Contract.</p> <p>10) A new Clause 36 shall be added as follows:</p> <p>36 Execution and Counterparts</p> <p>36.1 This Call-Off Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.</p> <p>36.2 Execution of this Call-Off Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Call-Off Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Call-Off Contract as if signed by each Party's manuscript signature. In such situation, this Call-Off Contract shall be formed on the date on which both Parties have electronically signed the Call-Off Contract as recorded in the Buyer's electronic contract management system.</p> <p>11) A new clause 37 shall be added as follows:</p> <p>37 Offshore Working</p> <p>The Buyer requires that no non-UK Supplier Staff be engaged in the delivery of the Services. Notwithstanding this requirement, the Buyer agrees to an exception permitting the Supplier to use its off-shore engineering staff based in India (the "Off-shore Resource") solely for software development, technical support and troubleshooting, and maintenance related to the Supplier's Services.</p> <p>The Supplier agrees that:</p> <ol style="list-style-type: none"> 1. Where possible, UK-based engineering staff will be used for technical support and troubleshooting that requires access to
--	---

the Buyer Data.

2. Where this is not possible (e.g. due to expertise and / or availability) and non-UK engineering staff are utilised then:
 - (a) this will be done under the direction of UK-based senior Supplier Staff;
 - (b) access by such staff will be time-limited to only such time as is strictly required to provide the relevant technical support and troubleshooting;
 - (c) the Supplier shall keep a full and complete audit log of non-UK engineering staff's access to the Service;
 - (d) such staff will only access the Buyer Data on the Service through the Supplier's UK Virtual Desktop Infrastructure (VDI);
 - (e) such staff will only have access to the Supplier's development and quality assurance (QA) environments unless the identification or remediation of the issue strictly requires access to the production environment;
 - (f) no Buyer Personal Data (or any Buyer Data which is Personal Data provided by or relating to the users of the Eligible Public Health Bodies) will be accessed, downloaded, stored or otherwise processed outside of the UK by the Offshore Resource other than in compliance with Data Protection Legislation and in accordance with section 13) below (Data Transfers).

12) Schedule 7 - Processing Data

- 12.1) Where the Supplier or its Sub-contractors (or any of its or their processors) act as a Processor of any Personal Data under this Call-Off Contract for the purposes of incorporating Schedule 7 of the Framework Agreement into this Call-Off Contract, paragraph 5(d) shall be deleted in its entirety and replaced with the following (provided that in respect of its Sub-contractors and Supplier's or their other processors, the Supplier shall procure materially equivalent obligations from such third parties as set out below):

- (d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data.

12.2) An extra row shall be added at the end of the table at Annex 1 of Schedule 7 (UK GDPR Information) as follows:

Jurisdiction of processing	UK
-----------------------------------	----

13) Data Transfers. Where the Supplier is acting as a Controller of any Personal Data under this Call-Off Contract, the Supplier (and its Subcontractors or processors) shall not transfer such Personal Data outside of the UK except where: (a) either the Supplier is transferring the Personal Data: (i) in accordance with Clause 37 (Off-shoring); or (ii) to the processors set out in Schedule 7; and (b) in each case, the following conditions are fulfilled:

- a. the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or
- b. the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which

	<p>could include relevant parties entering into the International Data Transfer Agreement (the "IDTA"), or International Data Transfer Agreement Addendum to the European Commission's SCCs ("the Addendum"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;</p> <ul style="list-style-type: none"> c. the Data Subject has enforceable rights and effective legal remedies; d. the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Buyer in meeting its obligations); and e. the transferring Party complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data.
<p>Personal Data and Data Subjects</p>	<p>Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1</p>
<p>Intellectual Property</p>	<p>Not Applicable</p>
<p>Social Value</p>	<p>Not Applicable</p>
<p>Performance Indicators</p>	<p>Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.</p>

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

Signatures:

KPMG LLP - 15 Canada Square, London, England, E14 5GL United Kingdom
Company number: OC301540
For and on behalf of the Supplier (KPMG LLP)

[REDACTED]

Full Name: [REDACTED]

Job Title/Role: KPMG PARTNER

Date Signed: 25-02-2025

NHS England - 7 & 8 Wellington Place Leeds, West Yorkshire Leeds LS1 4AP
For and on behalf of the Buyer (NHS England)

[REDACTED]

Full Name: [REDACTED]

Job Title/Role: Associate Commercial Director

Date Signed: 25 February 2025

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

Buyer Benefits

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

[G-Cloud 14 Buyer Benefit Record](#)

Annex A to the Order Form – Eligible Public Health Bodies

Eligible Public Health Bodies may include the following:

Arms Length Bodies

Care Quality Commission
Health Research Authority
Health Services Safety Investigations Body
Human Tissue Authority
Medicines And Healthcare Products Regulatory Agency (MHRA)
National Institute For Health And Care Excellence
NHS Blood And Transplant
NHS Business Services Authority
NHS Counter Fraud Authority
NHS England
NHS Resolution
The Human Fertilisation And Embryology Authority
UK Health Security Agency

Governmental Departments

Department of Health and Social Care (DHSC)

Integrated Care Boards (ICB)

NHS Bristol, North Somerset And South Gloucestershire Integrated Care Board
NHS Bath And North East Somerset, Swindon And Wiltshire Integrated Care Board
NHS Bedfordshire, Luton And Milton Keynes Integrated Care Board
NHS Birmingham And Solihull Integrated Care Board
NHS Black Country Integrated Care Board
NHS Buckinghamshire, Oxfordshire And Berkshire West Integrated Care Board
NHS Cambridgeshire And Peterborough Integrated Care Board
NHS Cheshire And Merseyside Integrated Care Board
NHS Cornwall And The Isles Of Scilly Integrated Care Board
NHS Coventry And Warwickshire Integrated Care Board
NHS Derby And Derbyshire Integrated Care Board
NHS Devon Integrated Care Board
NHS Dorset Integrated Care Board
NHS Frimley Integrated Care Board
NHS Gloucestershire Integrated Care Board
NHS Greater Manchester Integrated Care Board
NHS Hampshire And Isle Of Wight Integrated Care Board
NHS Herefordshire And Worcestershire Integrated Care Board
NHS Hertfordshire And West Essex Integrated Care Board
NHS Humber And North Yorkshire Integrated Care Board
NHS Kent And Medway Integrated Care Board
NHS Lancashire And South Cumbria Integrated Care Board
NHS Leicester, Leicestershire And Rutland Integrated Care Board
NHS Lincolnshire Integrated Care Board
NHS Mid And South Essex Integrated Care Board
NHS Norfolk And Waveney Integrated Care Board

NHS North Central London Integrated Care Board
NHS North East And North Cumbria Integrated Care Board
NHS North East London Integrated Care Board
NHS North West London Integrated Care Board
NHS Northamptonshire Integrated Care Board
NHS Nottingham And Nottinghamshire Integrated Care Board
NHS Shropshire, Telford And Wrekin Integrated Care Board
NHS Somerset Integrated Care Board
NHS South East London Integrated Care Board
NHS South West London Integrated Care Board
NHS South Yorkshire Integrated Care Board
NHS Staffordshire And Stoke-On-Trent Integrated Care Board
NHS Suffolk And North East Essex Integrated Care Board
NHS Surrey Heartlands Integrated Care Board
NHS Sussex Integrated Care Board
NHS West Yorkshire Integrated Care Board

Commissioning Support Units

NHS North Of England CSU
NHS Midlands and Lancashire CSU
NHS Arden And Greater East Midlands CSU
NHS South, Central and West CSU

NHS Trusts

Airedale NHS Foundation Trust
Alder Hey Children's NHS Foundation Trust
Ashford And St Peter's Hospitals NHS Foundation Trust
Avon And Wiltshire Mental Health Partnership NHS Trust
Barking, Havering And Redbridge Hospitals NHS Trust
Barnet, Enfield And Haringey Mental Health NHS Trust
Barnsley Hospital NHS Foundation Trust
Barts Health NHS Trust
Bedfordshire Hospitals NHS Foundation Trust
Berkshire Healthcare NHS Foundation Trust
Birmingham And Solihull Mental Health NHS Foundation Trust
Birmingham Community Healthcare NHS Foundation Trust
Birmingham Womens And Childrens NHS Foundation Trust
Black Country Healthcare NHS Foundation Trust
Blackpool Teaching Hospitals NHS Foundation Trust
Bolton NHS Foundation Trust
Bradford District Care NHS Foundation Trust
Bradford Teaching Hospitals NHS Foundation Trust
Bridgewater Community Healthcare NHS Foundation Trust
Buckinghamshire Healthcare NHS Trust
Calderdale And Huddersfield NHS Foundation Trust
Cambridge University Hospitals NHS Foundation Trust
Cambridgeshire And Peterborough NHS Foundation Trust
Cambridgeshire Community Services NHS Trust
Camden And Islington NHS Foundation Trust
Central And North West London NHS Foundation Trust
Central London Community Healthcare NHS Trust
Chelsea And Westminster Hospital NHS Foundation Trust

Cheshire And Wirral Partnership NHS Foundation Trust
Chesterfield Royal Hospital NHS Foundation Trust
Clatterbridge Cancer Centre NHS Foundation Trust
Cornwall Partnership NHS Foundation Trust
Countess Of Chester Hospital NHS Foundation Trust
County Durham And Darlington NHS Foundation Trust
Coventry And Warwickshire Partnership NHS Trust
Croydon Health Services NHS Trust
Cumbria, Northumberland, Tyne And Wear NHS Foundation Trust
Dartford And Gravesham NHS Trust
Derbyshire Community Health Services NHS Foundation Trust
Derbyshire Healthcare NHS Foundation Trust
Devon Partnership NHS Trust
Doncaster And Bassetlaw Teaching Hospitals NHS Foundation Trust
Dorset County Hospitals NHS Foundation Trust
Dorset Healthcare University NHS Foundation Trust
Dudley Integrated Health And Care NHS Trust
East And North Hertfordshire NHS Trust
East Cheshire NHS Trust
East Kent Hospitals University NHS Foundation Trust
East Lancashire Hospitals NHS Trust
East London NHS Foundation Trust
East Midlands Ambulance Service NHS Trust
East Of England Ambulance Service NHS Trust
East Suffolk And North Essex NHS Foundation Trust
East Sussex Healthcare NHS Trust
Epsom And St Helier University Hospitals NHS Trust
Essex Partnership University NHS Foundation Trust
Frimley Health NHS Foundation Trust
Gateshead Health NHS Foundation Trust
George Eliot Hospital NHS Trust
Gloucestershire Health And Care NHS Foundation Trust
Gloucestershire Hospitals NHS Foundation Trust
Great Ormond Street Hospital For Children NHS Foundation Trust
Great Western Hospitals NHS Foundation Trust
Greater Manchester Mental Health NHS Foundation Trust
Guy's And St Thomas' NHS Foundation Trust
Hampshire Hospitals NHS Foundation Trust
Harrogate And District NHS Foundation Trust
Herefordshire And Worcestershire Health And Care NHS Trust
Hertfordshire Community NHS Trust (Ry4)
Hertfordshire Partnership University NHS Foundation Trust
Homerton Healthcare NHS Foundation Trust
Hounslow And Richmond Community Healthcare NHS Trust
Hull University Teaching Hospitals NHS Trust
Humber Teaching NHS Foundation Trust
Imperial College Healthcare NHS Trust
Isle Of Wight NHS Trust
James Paget University Hospitals NHS Foundation Trust
Kent And Medway NHS And Social Care Partnership Trust
Kent Community Health NHS Foundation Trust
Kettering General Hospital NHS Foundation Trust
King's College Hospital NHS Foundation Trust
Kingston Hospital NHS Foundation Trust
Lancashire And South Cumbria NHS Foundation Trust

Lancashire Teaching Hospitals NHS Foundation Trust
Leeds And York Partnership NHS Foundation Trust
Leeds Community Healthcare NHS Trust
Leicestershire Partnership NHS Trust
Lewisham And Greenwich NHS Trust
Lincolnshire Community Health Services NHS Trust
Lincolnshire Partnership NHS Foundation Trust
Liverpool Heart And Chest Hospital NHS Trust
Liverpool University Hospitals NHS Foundation Trust
Liverpool Womens Hospital NHS Trust
London Ambulance Service NHS Trust
London North West University Healthcare NHS Trust
Maidstone And Tunbridge Wells NHS Trust
Manchester University NHS Foundation Trust
Medway NHS Foundation Trust
Mersey And West Lancashire Teaching Hospitals NHS Trust
Mersey Care NHS Foundation Trust
Mid And South Essex NHS Foundation Trust
Mid Cheshire Hospitals NHS Foundation Trust
Mid Yorkshire Teaching NHS Trust
Midlands Partnership NHS Foundation Trust
Milton Keynes University Hospital NHS Foundation Trust
Moorfields Eye Hospital NHS Foundation Trust
Norfolk And Norwich University Hospitals NHS Foundation Trust
Norfolk And Suffolk NHS Foundation Trust
Norfolk Community Health And Care NHS Trust
North Bristol NHS Trust
North Cumbria Integrated Care NHS Foundation Trust
North East Ambulance Service NHS Foundation Trust
North East London NHS Foundation Trust
North Middlesex University Hospital NHS Trust
North Staffordshire Combined Healthcare NHS Trust
North Tees And Hartlepool NHS Foundation Trust
North West Ambulance Service NHS Trust
North West Anglia NHS Foundation Trust
Northampton General Hospital NHS Trust
Northamptonshire Healthcare NHS Foundation Trust
Northern Care Alliance NHS Foundation Trust
Northern Lincolnshire And Goole NHS Foundation Trust
Northumbria Healthcare NHS Foundation Trust
Nottingham University Hospitals NHS Trust
Nottinghamshire Healthcare NHS Foundation Trust
Oxford Health NHS Foundation Trust
Oxford University Hospitals NHS Foundation Trust
Oxleas NHS Foundation Trust
Pennine Care NHS Foundation Trust
Portsmouth Hospitals University NHS Trust
Rotherham, Doncaster And South Humber NHS Foundation Trust
Royal Berkshire NHS Foundation Trust
Royal Cornwall Hospitals NHS Trust
Royal Devon University Healthcare NHS Foundation Trust
Royal Free London NHS Foundation Trust
Royal National Orthopaedic Hospital NHS Trust
Royal Papworth Hospital NHS Foundation Trust
Royal Surrey County Hospital NHS Foundation Trust

Royal United Hospitals Bath NHS Foundation Trust
Salisbury NHS Foundation Trust
Sandwell And West Birmingham Hospitals NHS Trust
Sheffield Children's NHS Foundation Trust
Sheffield Health & Social Care NHS Foundation Trust
Sheffield Teaching Hospitals NHS Foundation Trust
Sherwood Forest Hospitals NHS Foundation Trust
Shrewsbury And Telford Hospital NHS Trust
Shropshire Community Health NHS Trust
Solent NHS Trust
Somerset NHS Foundation Trust
South Central Ambulance Service NHS Trust
South East Coast Ambulance Service NHS Foundation Trust
South London And Maudsley NHS Foundation Trust
South Tees Hospitals NHS Foundation Trust
South Tyneside And Sunderland NHS Foundation Trust
South Warwickshire NHS Foundation Trust
South West London And St George's Mental Health NHS Trust
South West Yorkshire Partnership Foundation NHS Trust
South Western Ambulance Service NHS Trust
Southern Health NHS Foundation Trust
St George's University Hospitals NHS Foundation Trust
Stockport NHS Foundation Trust
Surrey And Borders Partnership NHS Foundation Trust
Surrey And Sussex Healthcare NHS Trust
Sussex Community NHS Foundation Trust
Sussex Partnership NHS Foundation Trust
Tameside And Glossop Integrated Care NHS Foundation Trust
Tavistock And Portman NHS Foundation Trust
Tees, Esk And Wear Valleys NHS Foundation Trust
The Christie NHS Foundation Trust
The Dudley Group NHS Foundation Trust
The Hillingdon Hospitals NHS Foundation Trust
The Leeds Teaching Hospitals NHS Trust
The Newcastle Upon Tyne Hospitals NHS Foundation Trust
The Princess Alexandra Hospital NHS Trust
The Queen Elizabeth Hospital King's Lynn NHS Foundation Trust
The Queen Victoria Hospital NHS Foundation Trust
The Robert Jones & Agnes Hunt Orthopaedic Hospital NHS Foundation Trust
The Rotherham NHS Foundation Trust
The Royal Marsden NHS Foundation Trust
The Royal Orthopaedic Hospital NHS Foundation Trust
The Royal Wolverhampton NHS Trust
The Walton Centre NHS Foundation Trust
Torbay And South Devon NHS Foundation Trust
United Lincolnshire Hospitals NHS Trust
University College London Hospitals NHS Foundation Trust
University Hospitals Birmingham NHS Foundation Trust
University Hospitals Bristol And Weston NHS Foundation Trust
University Hospitals Coventry And Warwickshire NHS Trust
University Hospitals Dorset NHS Foundation Trust
University Hospitals Of Derby And Burton NHS Foundation Trust
University Hospitals Of Leicester NHS Trust
University Hospitals Of Morecambe Bay NHS Foundation Trust
University Hospitals Of North Midlands NHS Trust

University Hospitals Plymouth NHS Trust
University Hospitals Southampton NHS Foundation Trust
University Hospitals Sussex NHS Foundation Trust
Walsall Healthcare NHS Trust
Warrington And Halton Hospitals NHS Foundation Trust
West Hertfordshire Hospitals NHS Trust
West London NHS Trust
West Midlands Ambulance Service University NHS Foundation Trust
West Suffolk NHS Foundation Trust
Whittington Health NHS Trust
Wirral Community Health And Care NHS Foundation Trust
Wirral University Teaching Hospital NHS Foundation Trust
Worcestershire Acute Hospitals NHS Trust
Wrightington, Wigan And Leigh Teaching Hospitals NHS Foundation Trust
Wye Valley NHS Trust
York And Scarborough Teaching Hospitals NHS Foundation Trust
Yorkshire Ambulance Service NHS Trust

GP Practices and Primary Care Networks (PCNs):

NHS England make lists of GP Practices and PCNs available at regular intervals, the link changes each time. The latest published list is linked:

<https://www.england.nhs.uk/wp-content/uploads/2023/03/PRN00157-january-2023-pcn-adjusted-populations-march-2023.xlsx>

Annex B to the Order Form – Service definition



KPMG – About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.



330+ professionals
15 office locations
Part of a global team of 6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.



Cyber strategy



Cyber risk



Cyber and enterprise resilience



Privacy compliance



Cyber tech transformation



Identity and access management



Cyber defence services



Cyber incident response

Our Cyber team is complemented by our Connected Technology team.

We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.



About CRI



Cyber Risk Insights Story

Our Cyber Risk Quantification (CRQ) capability started in Excel in 2016, with a combination of Power Query and Visual Basic. By 2022, we had productised 3 discrete excel models into a fully functional WebApp. This was used by our consulting teams as an enabler to deliver CRQ engagements to our clients. Fast forward another year to June 2023 with the mission of making CRQ accessible to all, we launched Cyber Risk Insights in the market as a licensable SaaS product.

Our approach to innovation is client-centric, building features which help answer our clients' most prominent cyber risk questions. Cyber Risk Insights was developed by a multidisciplinary team, including cyber security, data modelling, software engineering, cloud, econometrics, digital design and actuarial experts. It's this diverse team that bring these innovations to life alongside a powerful user experience in the product.



Product Features

- Executive dashboard for an aggregated view of risk exposure
- Data helpers to guide you through your analysis
- Areas for capturing likelihood and impact data
- Provides cyber risk exposure in a financial range and a supporting loss exceedance curve (LEC) visualisation
- Financial outputs covering average annualised loss exposure, most likely exposure, minimum (5th percentile), worst case (95th percentile) and 10th/0th percentiles.
- Recommends where to invest to maximises risk reduction
- Measure risk reduction through cost-benefit analysis of your initiatives
- Identifies strengths and weaknesses in your defences
- 12 out-of-the-box cyber threat scenarios that
- Threat-modelling capability for developing the attack paths for the scenarios relevant to your business
- Simulation analysis to test the effectiveness of defence mechanisms



KPMG Products

KPMG is a global organisation supporting businesses of all sizes, across all industries. In the UK, our 15,300 strong team support our clients through offering deep business, sector and technology experience. CRI is part of KPMG Products, a range of powerful tools and applications designed to increase the speed and accuracy of your decision-making

KPMG Products is the business behind KPMG's portfolio of digital assets, that we build & sell to clients. KPMG Products was created to bring new forms of growth to the firm. Particularly focussing on the building and selling of licensable SaaS solutions. KPMG's new product department harnesses KPMG's existing intellectual property, extensive datasets and consulting know-how. To create innovative, repeatable and scalable products that we take to market.



What is KPMG Cyber Risk Insights (CRI)?

CRI is a licensable SaaS product which takes a scenario-driven approach to more accurately assess the likelihood and impact of cyber-attacks. It uses powerful and intuitive dashboarding to show insights, with a strong user interface.

Key inputs	Cyber threat scenario modelling	Cyber capability effectiveness estimations	Attacker contact rate estimations	Financial impact estimations	Cyber investment data
Example insights	Prioritise cyber risks 		Optimise cyber spend 		Fix weaknesses in defences
					Identify optimal future improvements

Why use KPMG CRI?

CRI gives you a comprehensive view of the potential financial losses in the event of a cyber-attack, as well as the best 'bang for buck' investments to help mitigate those attacks. This allows you to make defensible and data-driven decisions and can help you prioritise your remediation efforts. The typical questions CRI helps answer are below.

<ul style="list-style-type: none"> Prioritise cyber risks Optimise cyber spend Improve communication Comply with regulation 	<p>Regulator(s) Board CEO CFO COO CIO CRO CISO Business</p> <p>What is our true risk exposure to cyber attack (likelihood in a year and potential financial impact)? Is it within our risk appetite? What cyber risks should we prioritise?</p>
	<p>Board CEO CFO COO CIO CRO CISO Business</p> <p>What cyber investments would deliver best bang-for-buck risk reduction? If we invest XM in cyber next year, is this too much or too little?</p>
	<p>Board CEO COO CIO CRO CISO Business</p> <p>I know cyber is a complex risk with many interdependencies – how can we simply explain our overall exposure in order to make effective well-informed decisions?</p>
	<p>Regulator(s) Board CEO CRO CISO</p> <p>How can I determine the potential 'material' impact of a cyber attack on my business? How can I communicate cyber risk to the Board to meet new cyber reporting requirements?</p>

How has CRI helped our clients?

Business case for investment

Healthcare

Enabled a national health organisation, to forecast the potential reduction in cyber risk exposure through executing on their multi-year cyber strategy.

- ✓ A baseline view of cyber risk exposure across Secondary Care, and forecasted risk reduction from the programme.
- ✓ National guidance documentation aligned to the National Cyber Security Centre Cyber Assessment Framework outcomes.
- ✓ Supported the central cyber risk management team on operationalising their cyber risk management lifecycle, enabled through risk quantification.

Prioritisation of a cyber roadmap

Insurance

A CISO was receiving Board-level challenge about the benefit of the cyber investment programme and was asked to reduce spend. CRI enabled:

- ✓ Identification of the priority controls for investment based on robust cost-benefit analysis.
- ✓ Demonstrable year-on-year reduction in cyber risk exposure tied to benefits tracking of change initiatives.
- ✓ Granular assessments of individual business units after the Group-wide assessment.

Managing exposure across a portfolio

Private Equity

Cyber risk assessment's and remediation plans were required across 20+ Portfolio Companies. CRI enabled:

- ✓ Each Portfolio Company to understand their cyber risk exposure, in financial terms.
- ✓ Each Portfolio Company to prioritise their cyber investments based on the specific threats to their business.
- ✓ The replacement of their 1-5 maturity assessment methodology, giving leaders better confidence in the security of their portfolio.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/uk/en/CRI

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure, please visit home.kpmg/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. Throughout this document, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

How can CRI help you?

Make the case to the board

CRI's logical and transparent approach helps you to communicate cyber risk to senior stakeholders, demonstrate the business benefits of cyber capabilities and make compelling investment cases.

Carry out systematic, consistent, data-driven assessments

CRI makes the adoption of quantitative techniques quick and simple and improves the objectivity of risk assessments by producing consistent, data-driven results.

Quantify likelihood and impact

Access to our tried and tested models, which quantify the likelihood of cyber-risk scenarios occurring, the possibility of attackers succeeding across the layers of defence and potential financial losses.

Target spend to reduce exposure

Graphical risk scenario models allow you to see where your cyber capabilities contribute to risk reduction across the layers of defence and which areas would benefit most from investment.

Help optimise investments

Determining the optimal investment portfolio of cyber capabilities, to help achieve a great return on investment in risk reduction.

Test investments

Estimate the payback period for an investment or investment portfolio, based on a cost-benefit analysis of spend compared to the expected reduction in cyber losses.

Service Details

Implementation Plan

Timescales are driven by a number of variables including the scale and complexity of each Customer's scope together with quality of data and availability of resources.

We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG Powered service would be agreed as part of the procurement of the service. As part of the service we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs.

Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop / articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement

Onboarding and offboarding support:

Onboarding...continued

- Provision of orientation sessions in the Powered Methodology, Powered assets, Platform principles, Powered Execution Suite tools to prepare clients teams for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account in change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a Project kick off event and associated materials to formally launch the project and to aid new joiners in orientation

The migration of client data is often a critical path item on the on boarding plan. We work with our clients to assist them to transition data to the new Platform. As part of this we would provide standard templates and knowledge transfer to allow the client and/or their existing service provider to extract and provide data in the correct format.

Offboarding:

Each implementation has a post go live ("Evolve phase") in which KPMG will provide post go live support working with each Clients Business as Usual (BAU) team to fully transition on going service delivery to the Clients' BAU support team according to the agreed plan.



Service Details

The levels of data backup and restore, and disaster recovery you'll provide, such as business continuity and disaster recovery plans.

KPMG has comprehensive business continuity and physical security procedures in place to cover its day to day and business operations.

The KPMG Business Continuity and Readiness Statement Executive summary dated November 2022 includes the following:

The Business Continuity team follow the Business Continuity Institute best practice guidelines and comply with the International Standard ISO22301: 2012.

The firm has ISO27001 accreditation, the scope of the external audit extended for the first time in 2010 to include the Business Continuity Management across the UK firm externally audited every six months.

Incident & Crisis Management response: role holders are trained and exercised.

Business Recovery Readiness:

Strategy

The firm's recovery strategy is based on the use of the KPMG UK office network to provide workplace and Information & Communications Technology contingencies in the event of the loss of one (or more) of the firm's offices.

The firm's business recovery strategy is based on using the offices throughout the UK as alternate site contingencies for building denial events with remote working at home and client site completing the response by leveraging KPMG's agile working capability: high capacity VPN, all staff have laptops and Smart phones.

Plans

Business Continuity Co-ordinators are responsible for the maintenance and execution of client service recovery plans.

The business recovery plans are reviewed within an ongoing programme of scenario based tabletop exercises.

The plans are maintained and centrally monitored using business continuity planning software. These plans are supported by the firm's infrastructure (ITS, Facilities and HR) support plans

Exercising

Business Recovery plans: exercised once every year.

Detailed audits of the content of all plans are completed annually

BCDR: Risk and Impact Mitigation:

KPMG has a three lines of defence Risk Governance model:

- i. Operational teams (ITS, HR, Physical Security etc) responsible for implementation of activities / adherence with policies and standards and day to day ownership & management of
- ii. Oversight - BCM as part of a wider Information Protection team within the Quality & Risk Management function defines strategy / policies, ensures compliance and provides assurance.
- iii. Independent Assurance – Internal Audit overseen by the Audit & Risk Committee, external audit (ISO27001 BCM audit on a biannual basis) and Client audits.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted IT infrastructure and business applications.

The primary and secondary data centres are dedicated data halls hosted in purpose built UI Tier III equivalent facilities. The buildings are separately owned by two of the market leaders in data centre colocation.

KPMG operates a twin data centre model, providing provision to manage disruptions affecting hosted IT infrastructure and business applications.

Service Details

BCDR Risk and Impact Mitigation, continued:

The data centres are sufficiently physically separated to minimise exposure to shared risk/threat occurrence, whilst within distances to support synchronous replication of data to minimise data loss opportunity in the event of DR.

Both facilities are located in the UK. Production IT systems are typically hosted on an active passive infrastructure design, providing high availability and managed failover between data centres, underpinned by resilient fibre links.

KPMG provides a disk to disk backup strategy supplemented by snapshot and clone solutions to provide the lowest RTO. Disk backups are replicated between data centres for additional assurance. Long term data retention is provided through a choice of archive disk or tape backup where required.

The KPMG network is fully resilient, with all offices linked by dual network paths into an MPLS Wide Area Network, providing connectivity to KPMG's Data Centres.

KPMG has several risk assessments for suppliers in place, which cover business continuity, health and safety and data security.

KPMG provides related consulting services to clients.

Pricing overview, including volume discounts or data extraction costs

Consulting Prices are as per the G Cloud 14 rate structure.

Projects can be charged using either Fixed Price and Time and Materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Typically, data extraction is addressed by clients with input from KPMG but we work closely with our clients to develop the data migration strategy and plan, providing templates with the target Platform format, to enable our clients to cleanse and map extracted data. We can apply varying levels of data migration automation techniques to address large volumes or complex requirements.

Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

Cloud software is updated regularly to apply minor fixes and to a schedule for more significant updates. These types of maintenance activities are usually well documented and pre advised by the Cloud software vendor and, where notified, are considered in project planning and particularly design and regression testing activities.

Customisation:

Our approach is to 'configure rather than customise', adopting standard Cloud software functionality to enable ease of upgrade and to take advantage of new updates and releases with minimal issues. Most Cloud software vendors restrict the capability to customise the core application as it impacts on the ability to service and support a common code base and the associated financial model.



Service Details

Service levels like performance, availability and support hours

Not Applicable

Service levels like performance, availability and support hours

The service levels and support hours for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

The ordering and invoicing process

The ordering process for G Cloud services is laid out in the 'G Cloud buyers' guide on the www.gov.uk website.

Invoicing arrangements will be as per the agreed G Cloud order form and will vary from engagement to engagement.

How buyers or suppliers can terminate a contract:

Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- convenience,
- failure to remedy a material breach and
- insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.

Any technical requirements

Each Cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for the majority of organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the Services. Microsoft Office 365 & Teams are used by all colleagues within the firm, with other tools such as Jira and Confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.



kpmg.com/uk

This proposal is made by KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. The proposals set out in this document do not constitute an offer capable of acceptance. They are in all respects subject to satisfactory completion of KPMG's procedures to evaluate prospective clients and engagements, including independence and conflict checking procedures and, the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International and its related entities provide no services to clients. No member firm has any authority to obligate or bind KPMG International, any of its related entities or any other member firm vis-à-vis third parties, nor does KPMG International or any of its related entities have any such authority to obligate or bind any member firm.

© 2024 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document classification: KPMG Public

Part B: Terms and conditions

1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months.

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)

30 (Insurance)
31 (Severability)
32 and 33 (Managing disputes and Mediation)
34 (Confidentiality)
35 (Waiver and cumulative remedies)
36 (Corporate Social Responsibility)
paragraphs 1 to 10 of the Framework Agreement Schedule 3

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' or to 'CCS and/or the Buyer' 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

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

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

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

3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

- 4.1 The Supplier Staff must:
 - 4.1.1 be appropriately experienced, qualified and trained to supply the Services
 - 4.1.2 apply all due skill, care and diligence in faithfully performing those duties

- 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
- 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 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:
 - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract

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

6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

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

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
- 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
 - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

10. Confidentiality

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

11. Intellectual Property Rights

- 11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.
- 11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.
- 11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance

with this Contract, including the right to grant sub-licences to Subcontractors provided that:

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

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

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

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

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim: alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law; alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party; arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

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

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

rights granted to the Buyer under this Call-Off Contract

Supplier's performance of the Services

use by the Buyer of the Services

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

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

11.8 Clause 11.6 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

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security - Classification policy:

<https://www.gov.uk/government/publications/government-security-classifications>

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

<https://www.npsa.gov.uk/sensitive-information-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

<https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

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

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

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

15. Open source

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

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
 - 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
 - 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

7 (Payment, VAT and Call-Off Contract charges)

8 (Recovery of sums due and right of set-off)

9 (Insurance)

10 (Confidentiality)

11 (Intellectual property rights)

12 (Protection of information)

13 (Buyer data)

19 (Consequences of suspension, ending and expiry)

24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),

24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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.

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

20. Notices

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

Manner of delivery: email

Deemed time of delivery: 9am on the first Working Day after sending

Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer
 - 21.6.2 there will be no adverse impact on service continuity
 - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
 - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
- 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
 - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
 - 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
 - 21.8.4 the testing and assurance strategy for exported Buyer Data
 - 21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations
 - 21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

- 22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
- 22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
 - 22.1.2 other information reasonably requested by the Buyer
- 22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.
- 22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

- 23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.
- 23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.
- 23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

- 24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).
- 24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:
 - 24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and
 - 24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.
- 24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).
- 24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

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

- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.
- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.
- 25.4 This clause does not create a tenancy or exclusive right of occupation.
- 25.5 While on the Buyer's premises, the Supplier will:
 - 25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises
 - 25.5.2 comply with Buyer requirements for the conduct of personnel
 - 25.5.3 comply with any health and safety measures implemented by the Buyer
 - 25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
- 25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

- 26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.
- 26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.
- 26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

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

- 27.1 Except as specified in clause 29.8, a person who is not a Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its

terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

- 28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.
- 28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
 - 29.2.1 the activities they perform
 - 29.2.2 age
 - 29.2.3 start date
 - 29.2.4 place of work
 - 29.2.5 notice period
 - 29.2.6 redundancy payment entitlement
 - 29.2.7 salary, benefits and pension entitlements
 - 29.2.8 employment status
 - 29.2.9 identity of employer
 - 29.2.10 working arrangements
 - 29.2.11 outstanding liabilities
 - 29.2.12 sickness absence
 - 29.2.13 copies of all relevant employment contracts and related documents
 - 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

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

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.

The Supplier will cooperate 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.

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

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

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

30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
 - 31.2.1 work proactively and in good faith with each of the Buyer's contractors

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

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 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 using the template in Schedule 9. This includes any changes in the Supplier's supply chain.
- 32.3 If either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

Access to the Cyber Risk Insights platform

- Ability to continually update your insights with latest business data
- Access to Industry Insights to support your assessment
- Unlimited assessments ⁽¹⁾ ⁽³⁾
- Benchmark assessments against your industry
- Create custom threat scenario models
- Access to email and telephone support through our Helpdesk ⁽²⁾
- Access to a dedicated customer success manager
- Access to our Knowledge Base to support your users

(1) An assessment refers to the scope a user of CRI will conduct their quantitative risk assessment on, for example, a business unit.

(2) Email and telephone support is available between 09:00 – 17:00 (UK time) Monday to Friday excluding bank holidays and public holidays in England.

(3) Fair usage and technical restrictions may apply.

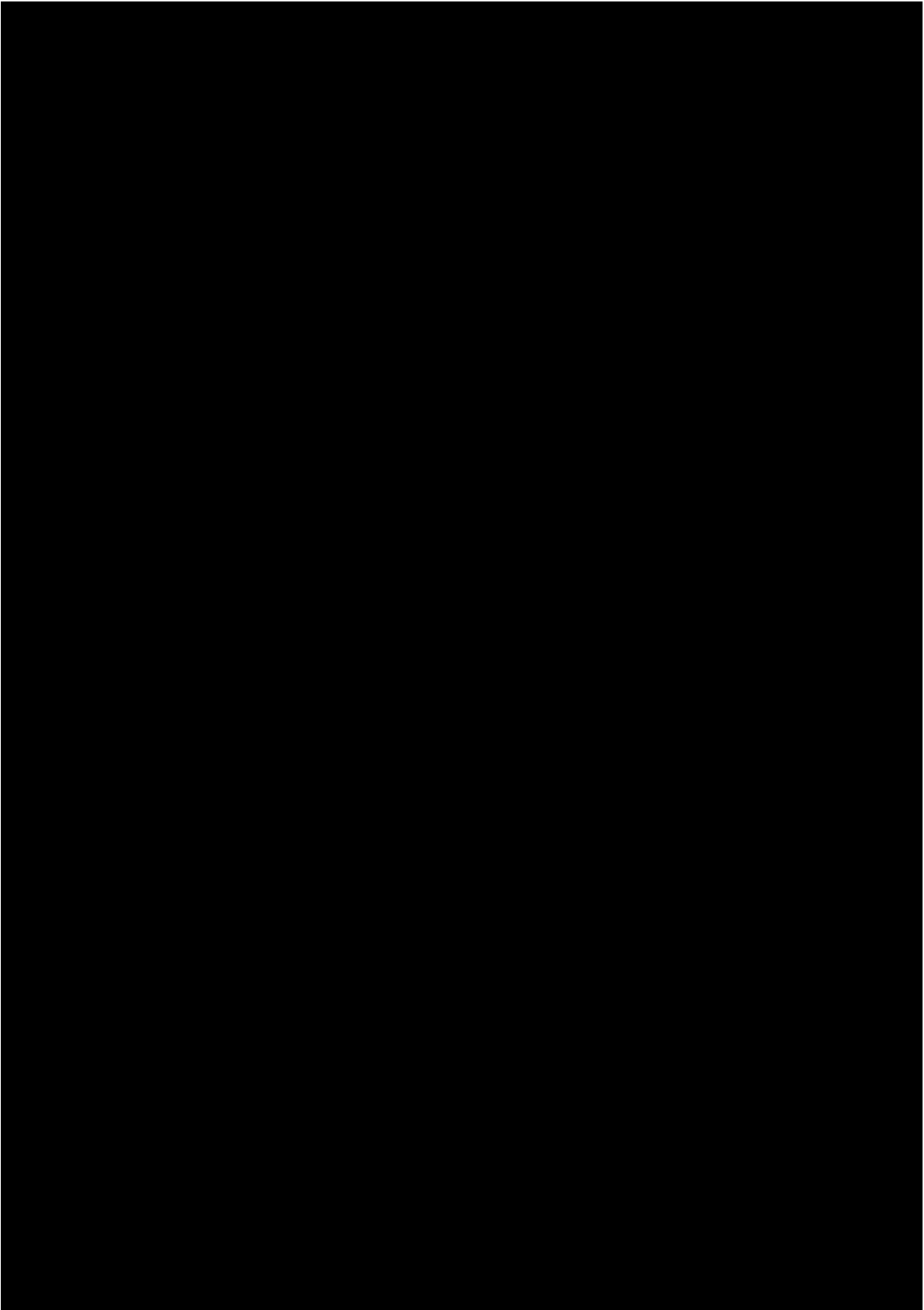
Schedule 2: Call-Off Contract charges

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

Cyber Risk Insights Enterprise license – Platinum, as described below in the 'Pricing' section.

Quantity: Unlimited Seats

Cost Breakdown: £192,593 (ex VAT) for 26 months



Schedule 3: Collaboration agreement

NOT USED

Collaboration Agreement Schedule 2 [Insert Outline Collaboration Plan]

NOT USED

Schedule 4: Alternative clauses

1. Introduction

- 1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

- 2.1 The Buyer may, in the Order Form, request the following alternative Clauses:
 - 2.1.1 Scots Law and Jurisdiction
 - 2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.
 - 2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.
 - 2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FOIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.
 - 2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.
 - 2.1.6 References to "tort" will be replaced with "delict" throughout
- 2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:
 - 2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)
- 2.3 Discrimination
 - 2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:
 - Employment (Northern Ireland) Order 2002
 - Fair Employment and Treatment (Northern Ireland) Order 1998
 - Sex Discrimination (Northern Ireland) Order 1976 and 1988
 - Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
 - Equal Pay Act (Northern Ireland) 1970
 - Disability Discrimination Act 1995
 - Race Relations (Northern Ireland) Order 1997
 - Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
 - Employment Equality (Age) Regulations (Northern Ireland) 2006

Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
The Disability Discrimination (Northern Ireland) Order 2006
The Employment Relations (Northern Ireland) Order 2004
Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
Employment Relations (Northern Ireland) Order 2004
Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

persons of different religious beliefs or political opinions
men and women or married and unmarried persons
persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
persons of different ages
persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

the issue of written instructions to staff and other relevant persons
the appointment or designation of a senior manager with responsibility for equal opportunities
training of all staff and other relevant persons in equal opportunities and harassment matters
the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of:

the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards

which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

- 2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.
- 2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.
- 2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.
- 2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

2.7 Criminal damage

- 2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).
- 2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.
- 2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.
- 2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

NOT USED

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

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

Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>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</p> <p>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.</p>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7

<p>Force Majeure</p>	<p>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</p> <p>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</p>
<p>Former Supplier</p>	<p>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).</p>
<p>Framework Agreement</p>	<p>The clauses of framework agreement RM1557.14 together with the Framework Schedules.</p>
<p>Fraud</p>	<p>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.</p>

Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

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

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium a Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) 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 (b) 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 (c) all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: the supplier's own limited company a service or a personal service company a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of
-----------------	---

	know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.

Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.
Prohibited act	<p>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:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> under the Bribery Act 2010 under legislation creating offences concerning Fraud at common Law concerning Fraud committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data.

Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:</p> <ul style="list-style-type: none"> details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract; details of the cost of implementing the proposed variation; details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; a timetable for the implementation, together with any proposals for the testing of the variation; and such other information as the Buyer may reasonably request in (or in response to) the variation request;

Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

Schedule 7: UK GDPR Information

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

Annex 1 - Processing Personal Data

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

- 1.1.1.1 The contact details of the Buyer’s Data Protection Officer are: **Data Protection Officer**, england.dpo@nhs.net
- 1.1.1.2 The contact details of the Supplier’s Data Protection Officer are: **Data Protection Officer**, dataprivacy@kpmg.co.uk.
- 1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p>The Parties are Independent Controllers of Personal Data</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> - <i>Business contact details shared between them in the course of ordinary correspondence (“Business Contact Details”).</i> - <i>User access details of Buyer Personnel and Eligible Public Health Body Personnel who are users of Cyber Risk Insights platform collected for the purpose of user access control to the Platform and usage logging (“User Access Details”).</i>
Duration of the Processing	<p><i>Upon termination or expiry of this Call-Off Contract</i></p>
Nature and purposes of the Processing	<p><i>The nature of the processing covers:</i></p> <p><i>In respect of the Business Contact Details:</i></p> <ul style="list-style-type: none"> - <i>enable the administration and implementation of the contract to design, build and develop the Platform</i>

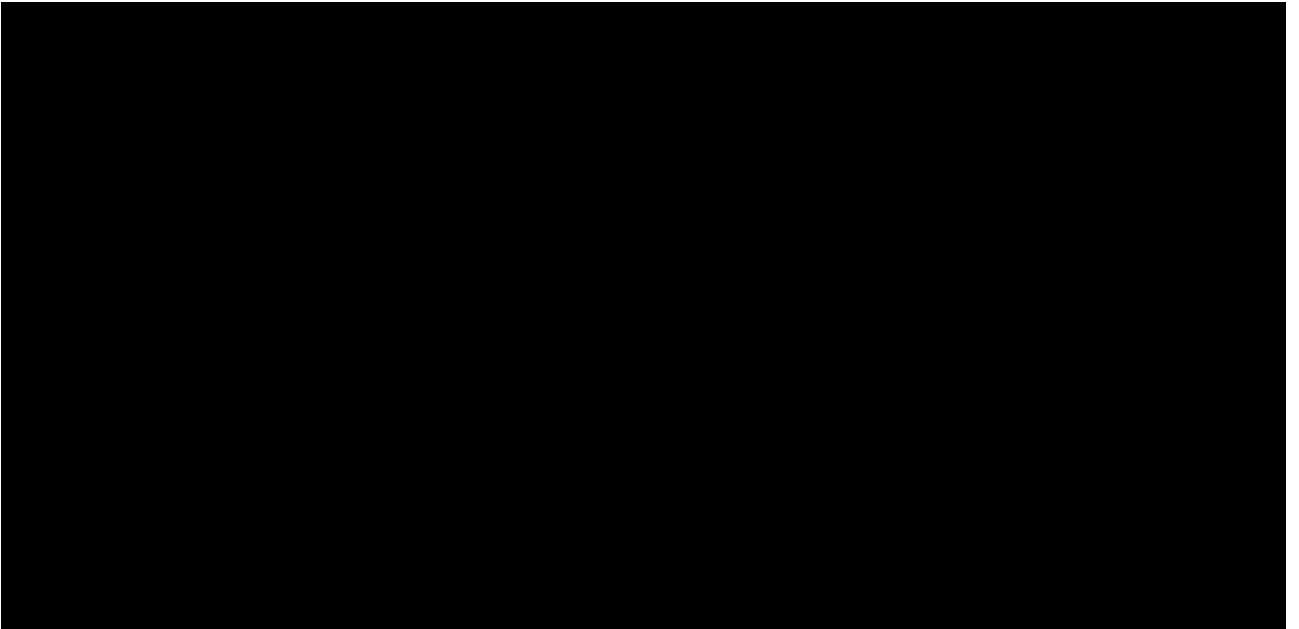
	<p>- <i>communicating with stakeholders concerning their use of the Service</i></p> <p><i>In respect of the User Access Details</i></p> <ul style="list-style-type: none"> - <i>User access control and usage logging.</i>
Type of Personal Data	<p><i>Business Contact Details</i></p> <ul style="list-style-type: none"> - <i>Names</i> - <i>Job titles</i> - <i>Email address</i> - <i>Telephone number</i> - <i>Employer</i> <p><i>User Access Details</i></p> <ul style="list-style-type: none"> - <i>Name</i> - <i>Email Address</i> - <i>Telephone number</i>
Categories of Data Subject	<p><i>Staff including temporary/agency/bank/secondment across health and care sector e.g. including NHSE, DHSC, NHS Providers, Local Authorities and Adult Social Care Providers, suppliers.</i></p>
International transfers and legal gateway	<p><i>No international transfers shall take place between the parties.</i></p> <p><i>Transfers of Buyer Personal Data by Supplier to the Offshore Resource shall be made under the SCCs (as adopted by the ICO).</i></p> <p><i>Transfers of Buyer Personal Data to the processors below outside of the UK and EU shall be made under the SCCs (as adopted by the ICO).</i></p>
Plan for return and destruction of the data once the Processing is complete	<p><i>Supplier will retain the personal data only for such period as it has a lawful basis to process such data in respect of the provision of the Service under this Call-Off Contract, after which it will securely delete such personal data from its systems in accordance with any retention periods set out in the Offboarding section of the Order Form.</i></p>

Processors

The Supplier shall: (a) remain fully liable for all acts or omissions of any of its Processors; and (b) only use (subject to the rest of this paragraph) the Processors listed in the table below in respect of the Processing of Buyer Personal Data. In the event that the Supplier wishes to add or change any Processor, the Supplier must:

- (a) at least 45 days in advance of allowing the Processor to Process any Buyer Personal Data, notify the Buyer in writing ("**Change of Processor Notice**") (by email to england.cyberimprovement@nhs.net, marked for the attention of 'Risk & Data workstream') of the intended Processor, its location, Processing, indicating that the Buyer should raise any objections within 25 days of receipt of the notice;

- (b) provide the Buyer with such information regarding the Processor as the Buyer may reasonably require;
- (c) enter into a written agreement with the Processor which meets the Supplier's obligations as a Controller and its data protection obligations under this Call-Off Contract;
- (d) in the event that the Buyer objects to the Processor, promptly enter into discussions with the Buyer and use all reasonable endeavours (acting in good faith) to come to an agreeable resolution with the Buyer. If such resolution is not reached (or if the Buyer does not object to the Processor) within 45 days of the receipt of the Change of Processor Notice then:
 - (i) the Supplier shall be entitled to use the new Processor (subject to the other data protection provisions of this Call-Off Contract); and
 - (ii) the Buyer shall be entitled to End this Call-Off Contract immediately on notice to the Supplier.



Annex 2 - Joint Controller Agreement

NOT USED

Schedule 8 (Corporate Resolution Planning)

NOT USED

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	[insert name of Buyer] ("the Buyer") And [insert name of Supplier] ("the Supplier")	
Contract name:	[insert name of contract to be changed] ("the Contract")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete] as applicable: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
A Variation Impact Assessment shall be provided within:	[insert number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: [Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

Words and expressions in this Variation shall have the meanings given to them in the Contract.

The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature (Buyer)

Date

Name (in Capitals)

Address

.....
.....
.....
.....
.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature (Supplier)

Date

Name (in Capitals)

Address

.....
.....
.....
.....