



# Crown Commercial Service

## G-Cloud 12 Call-Off Contract

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

Part A: Order Form .....	2
Schedule 1: Services .....	12
Schedule 2: Call-Off Contract charges .....	12
Part B: Terms and conditions .....	13
Schedule 3: Collaboration agreement .....	32
Schedule 4: Alternative clauses .....	44
Schedule 5: Guarantee .....	49
Schedule 6: Glossary and interpretations .....	57
Schedule 7: GDPR Information .....	68

## Part A: Order Form

<b>Digital Marketplace service ID number</b>	<b>875602076621030</b>
<b>Call-Off Contract reference</b>	Con_19098
<b>Call-Off Contract title</b>	Crime Programme Live Services Support and Production Management
<b>Call-Off Contract description</b>	Live Services Support and Production Management
<b>Start date</b>	24/05/2021
<b>Expiry date</b>	24/05/2023
<b>Call-Off Contract value</b>	£8,650,008
<b>Charging method</b>	Fixed Price for core services  Optional Workpackages pricing mechanism to be agreed by the parties

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

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

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

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

<b>From the Buyer</b>	The Secretary of State for the Ministry of Justice  102 Petty France  London  SW1H 9AJ
-----------------------	--

<b>To the Supplier</b>	Methods Business and Digital Technology Limited  Saffron House,  6-10 Kirby Street,  London,  England,  EC1N 8TS  Company number 02485577
<b>Together the ‘Parties’</b>	

## Principal contact details

### For the Buyer:

Title: Senior Contract Manager

Name: REDACTED

Email: REDACTED @justice.gov.uk

### For the Supplier:

Title: Executive Director

Name: REDACTED

Email: REDACTED @methods.co.uk

## Call-Off Contract term

<b>Start date</b>	This Call-Off Contract Starts on <b>24<sup>th</sup> May 2021</b> and is valid for <b>24 months</b> .
-------------------	--

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

<b>G-Cloud lot</b>	<p>This Call-Off Contract is for the provision of Services under:</p> <ul style="list-style-type: none"> <li>• Lot 3: Cloud support</li> </ul>
--------------------	--

<p><b>G-Cloud services required</b></p>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> <li>• GCloud Service Code 875602076621030 (Cloud Engineering and Support )</li> <li>• Including :-</li> <li>• Production (LIVE) 2nd line application and infrastructure support for Common Platform, Identity &amp; Access Management (IDAM) for CRIME, Magistrates Court Rota and Atlassian (infrastructure build and maintenance), to include all deployments into Production to agreed schedules.</li> <li>• Interaction and co-ordination with all 1st line Service Desk and 3rd Line Application Production Enhancement Teams (PET). See Annex A for the IT Support Model.</li> <li>• Interaction with all external 3rd party support services covering external connectivity with interim and /or in place Operational Working Agreements</li> <li>• Engagement with Cloud Hosting provider technical teams. The current provider is Microsoft Azure.</li> <li>• All activities pertaining to the support, maintenance and release of features/code into Production (Business Assurance, Pre-Production, Production, Non-Live and Live Management tiers and Live external connectivity zone).</li> <li>• Support and maintenance of Non-Live Management tier together with Non-live external connectivity zones.</li> <li>• Provisioning, support and maintenance of a parallel Production environment for Common Platform (to achieve a Blue/Green implementation), subject to necessary and timely Architecture and PDG approvals</li> <li>• Management, maintenance and support of all firewalls, security and perimeter devices.</li> <li>• Azure Active Directory and RBAC access/account and user device connectivity management for development/feature teams. This includes onboarding users into the non-live and live environments with appropriate access, and offboarding (remove all associated access) when they leave.</li> <li>• Providing technical infrastructure architecture services to liaise with the Programme architecture team. Create and maintain documentation on the infrastructure (Live and Non-Live) plus provide technical guidance for new features implementations and capabilities such as (but not limited too) interface design, infrastructure (IaaS and PaaS), network, security, network, scaling/resiliency or disaster recovery.</li> <li>• All active monitoring, alerting and log aggregation for all in scope services and Infrastructure for Non-Live and Live zones.</li> <li>• Ensure all processes and procedures are fully documented and kept up to date.</li> </ul>
---	---

- Creating/keeping documentation, Wiki pages, service manuals, instructions and any other artefacts relating to the supported services up to date/relevant.
- Maintenance and support of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) components in the Live zone.
- End to end Hosting Cost reporting for all Non-Live and Live environments.
- Management and operation of Live zone CI/CD infrastructure and associated repositories, including build and release pipelines.
- Continual improvement in support of all LIVE services, working with other programme and BAU teams as required.
- Work with the DTS Platform Operations Team to standardise practices, processes, infrastructure and components across all HMCTS Platforms; ensuring best practice is implemented and maintained.
- Liaison with the Programme design and development practises for matters Non-Live & Live infrastructure and Live Services.
- Liaison with DTS Service Management and processes e.g. Incident, Problem, Change management, Governance groups and Cyber Security functions.
- Investigation and resolution of incidents or problems created from Live Services (where applicable to 2nd Line Support).
- Keeping ITSM tooling (currently ServiceNow) up to date and relevant to the Live Services.
- Ensuring security standards are followed in all Non-Live and Live environments and implementing/applying fixes where vulnerabilities have been identified by the Programme or wider teams.
- Ensuring all software, services and utilities used by the Live Services follow/stay in line with the principles set within the Programme.
- Collaborating and working closely with the existing Non-Live DevOps team on delivering changes and releases into the Live Services.
- Support/fulfilling requests for data, logs and services to aid development or issue resolution.
- Provide handover and knowledge transfer to personnel within the Programme or DTS.
- All personnel with access to productions systems and live data and/or information are to hold a minimum of UK SC level Clearance. All other personnel to hold a minimum of BPSS clearance.

<b>Additional Services</b>	<b>As agreed between the parties in Work Packages using the rates outlined in Table 2 of Schedule 2</b>
<b>Location</b>	The Services will be delivered primarily to Ministry of Justice sites at 102 Petty France, London and Southern House, Wellesley Grove, Croydon.
<b>Quality &amp; Technical standards:</b>	<p>The quality and technical standards used as a requirement for this Call-Off Contract are :-</p> <ul style="list-style-type: none"> <li>• Government Digital Service (GDS) standards</li> <li>• HMCTS and Reform Security Policies and Procedures</li> <li>• HMCTS, Reform &amp; DACS Architecture Governance, Process and procedures</li> <li>• Reform Software Engineering Process and procedures</li> </ul> <p>The level of security clearance for this requirement is SC Clearance, for roles that access Production systems, data and information stored in documentation or other means of holding content (videos, wiki pages, etc). All other personnel to hold a minimum of BPSS clearance.</p>
<b>Service level agreement:</b>	<p>The service level and availability criteria required for this Call-Off Contract are :-</p> <ul style="list-style-type: none"> <li>• Service Support Hours are Monday to Saturday: 08:00 – 20:00</li> <li>• On Call/Out of Hours support are Monday - Saturday 20:00 - 08:00 and Sunday 24 hours.</li> </ul> <p>Specific Service levels and KPIs are detailed in this Part A Order Form and Schedule 1</p>
<b>Onboarding</b>	<p>The onboarding plan for this Call-Off Contract is outlined in the transition plan.</p> <div style="text-align: center;">  <p>TransitionPlan.pdf</p> </div>

<b>Offboarding</b>	The offboarding plan for this Call-Off Contract will be developed by the supplier by 18 <sup>th</sup> February 2022, and be kept regularly up to date.
<b>Collaboration agreement</b>	Not applicable
<b>Limit on Parties' liability</b>	<p>The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p>
<b>Insurance</b>	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• a minimum insurance period of 6 year following the expiration or Ending of this Call-Off Contract</li> <li>• professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)</li> <li>• employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law</li> </ul>
<b>Force majeure</b>	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.



<b>Audit</b>	Clauses 7.4 to 7.13 of the Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.
<b>Buyer's responsibilities</b>	<p>The Buyer is responsible for :-</p> <ul style="list-style-type: none"> <li>• Granting access to the Buyer's systems</li> <li>• Granting access to the Buyer's premises where required</li> <li>• Access to existing knowledge, artefacts and information required by the Supplier to deliver the Services</li> <li>• Providing and agreeing architectural designs and approvals required by the Supplier to deliver the Services</li> <li>• Providing prompt notifications and alerts of incidents and information required by the Supplier to deliver the Services</li> </ul>
<b>Buyer's equipment</b>	<p>The Buyer's equipment to be used with this Call-Off Contract includes :-</p> <p>The Buyers existing systems for delivering the Services</p>

### Supplier's information

<b>Subcontractors or partners</b>	<p>The following is a list of the Supplier's Subcontractors or Partners.</p> <p>Scrumconnect Limited.</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.

<b>Payment method</b>	The payment method for this Call-Off Contract is Fixed Price for the core Services as detailed in Schedule 1 and Schedule 2. Optional Workpackages pricing mechanism to be agreed by the parties.
<b>Payment profile</b>	The payment profile for this Call-Off Contract is <b>monthly</b> in arrears.
<b>Invoice details</b>	The Supplier will issue electronic invoices <b>monthly</b> in arrears. The Buyer will pay the Supplier within <b>30</b> days of receipt of a valid invoice.
<b>Who and where to send invoices to</b>	Invoices will be sent to <a href="mailto:APinvoices-CTS-U@sscl.gse.gov.uk">APinvoices-CTS-U@sscl.gse.gov.uk</a> .
<b>Invoice information required</b>	All invoices must include PO Number, Contract Reference (Con_19098), Project Ref (Crime Programme Live Services Support and Production Management), and Workpackage number if relevant
<b>Invoice frequency</b>	Invoice will be sent to the Buyer monthly.
<b>Call-Off Contract value</b>	The total value of this Call-Off Contract is £8,650,008.
<b>Call-Off Contract charges</b>	The breakdown of the Charges is £ REDACTED per calendar month for the core Services.

## Additional Buyer terms

<b>Guarantee</b>	Not Used
------------------	----------

<b>Warranties, representations</b>	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that that they are able to deliver the capabilities as set out in Schedule 1 and responded to in Schedule 2.
<b>Supplemental requirements in addition to the Call-Off terms</b>	Not Used
<b>Alternative clauses</b>	Not Used
<b>Supplier Responsibilities</b>	<p><b>Supplier Responsibilities</b></p> <p>The Supplier shall in performance, or as part of, the Services:</p> <ol style="list-style-type: none"> <li>1.Co-operate with the Buyer in all matters relating to the provision of its Services under this Agreement;</li> <li>2. Discharge its obligations under this Agreement using Personnel of requisite skill, experience and qualifications with all due skill care and diligence;</li> <li>3. Conform with all reasonable requirements of the buyer with regards to completion and conduct of the service;</li> <li>4.Consult and liaise with third parties including, without limitation, the Government Digital Service and the departmental Buyers incumbent IT suppliers for legacy systems when necessary or as reasonably required by the Buyer;</li> <li>5.Keep and make available to the Buyer accurate records of all development, coding and other work carried out in connection with the Services, copies of any or all materials and documents and any data under the Supplier's control which is or has been produced or used in connection with the Services.</li> <li>6.Provide the Services using the Buyer's choice of strategic software tools. Use of alternative software tools must be reviewed and approved in advance by the Buyer and must not result in any additional cost to the Buyer.</li> <li>7.The Supplier shall not, and shall ensure that its Personnel shall not, use any equipment, hardware, software, network or system of the Buyer for any purpose without the Buyer's express prior consent. Such express consent is given for use in connection with the performance of the Services</li> </ol>

<b>Public Services Network (PSN)</b>	Not Used
<b>Personal Data and Data Subjects</b>	Annex 1 of Schedule 7 is being used

## Performance of the Service and Deliverables

Suppliers shall deliver the following requirements:

### General

- Provide the authority with management function for Production support teams that includes the ability to meet the business critical services Service Level Targets for response and resolution for both operational and security incidents (see KPIs in section below).
- Target to deploy releases as scheduled in the Release plan for each of the Common Platform, Rota and IDAM services. The expectation is to deliver 1 patch release and 1 major release per week. All deployments subject to meeting HMCTS Digital and Technology Services (DTS) acceptance into live criteria. The releases (major and minor) take place outside of the standard in scope service hours.
- Chair the daily morning Release planning call (30mins) and fortnightly SDLC Group (1 hour). Track and report on progress of Release Candidates through the SDLC and dates for Production deployment.
- Engage programme, development, delivery and product enhancement teams to continually review and understand plans to identify resourcing requirements.
- Continual review and implement improvements to Monitoring and Alerting for all Live Services.
- Engage with 3<sup>rd</sup> party support vendors (including Azure Technical Teams and Account Management) to ensure a holistic support approach is achieved and maintained.
- Liaise with the Programme Technical Architects on a weekly basis to discuss any newly identified Interfaces or changes to existing Interfaces and infrastructure changes.
- Regular OS and vendor patching to agreed policy and procedures together with remediation activities of all security vulnerabilities as identified by Cyber Security.
- Represent Crime Programme at various DTS governance boards and ensure adherence to DTS governance for all SDLC and Platform infrastructure designs, changes and operations.
- Liaise with the relevant DTS Transition Managers for each Interface to discuss progress, issues, new release dates and develop plans and timelines. Record outcomes and progress.
- Produce, submit and obtain agreement with the authority changes to supplier resource, including volumes and skillsets.
- Monitoring of LIVE and Management layer product vendor roadmaps and announcements to identify upgrades and end of support/life dates.
- Plan and implement upgrades for Live and Management layer products to keep in line with Programme guidelines (N-1) and end of support/life dates.
- Document all interface requirements including but not limited to:

- a. Systems – with associated owners, suppliers, commercial arrangements, support and user groups, designs, architecture and test specifications
  - b. Compliance with Architectural designs
  - c. Configuration artefacts, such as IP address and system credentials
- Provide regular reports on business usage of environments including hosting costs and environment, application and infrastructure performance, availability, capacity and maintenance status.
- Provide the Authority with all relevant information pertaining to account management and technical input to monthly commercial reporting and performance reviews.
- Provide weekly reports on infrastructure and application availability, capacity and network and tooling performance.
- Provide information, documentation, knowledge transfer and training to HMCTS Digital and Technology Service support staff.
- Database administration and performance tuning along with the Programme architecture team, development and Non-Live DevOps team.

## **Environments and Live Services Support**

- Engage with DTS support functions (Crime IT Support, DTS Service Desk and PET teams) and Crime programme and DTS 3<sup>rd</sup> line to provide a coherent end to end 2<sup>nd</sup> line application and infrastructure support operation for the business. Respond to Live service support tickets as assigned in the ITSM tooling (currently ServiceNow).
- Respond to incidents and alerts, recording all Root Cause Analysis and response actions in ServiceNow, ensuring that the appropriate Business Service availability is maintained. For Priority 1 incidents, investigations and remediation is to continue through to resolution.
- Incident management for all incidents and issues, including working with DTS Major Incident Management, until resolution.
- Monitoring of Production applications and infrastructure (this refers to Pre-Production & Production environments and Management layer throughout this document unless specified), product vendor roadmaps and announcements to identify upgrades and end of support/life dates for 3<sup>rd</sup> party application tier tooling.
- Direct management and support of Non-Live and Live Management Tiers, Business Assurance and Pre-Production and Production environments, together with any future 'Live service' production environments on commissioning, subject to appropriate pre-acceptance testing. Maintaining appropriate levels of security segregation between Live and Non-Live environments.
- Commissioning, support and maintenance of a parallel Production environment (to achieve a Blue/Green setup) for Common Platform as guided by the Programme and associated design functions.
- Engage programme development, delivery and product enhancement teams to continually review and understand development activities in order to confirm that all skills and knowledge required to deploy and support both future application infrastructure & services are identified as early as possible.
- Provide support to the automated build, test & deployment of approved infrastructure & tooling in all Production environments. This includes delivery of automated network, storage, firewall, routing, load balancer, and VPN provisioning where necessary (such as for access to Non-Live and Live environments).
- Identify, document then conduct monitoring, checking and routine maintenance on infrastructure, Serverless and PaaS services in accordance with vendor, delivery teams or industry best practice. Automation is to be used as a standard approach.

- Implement and operate designed backup and recovery and DR solutions (when available) to agreed schedule within the overall agreed in-scope support hours.
- Propose, design and document any management application and application tooling upgrades, improvements and end of support/life replacements. These are to be submitted via the appropriate Programme/DTS governance for approval.
- Provide input and recommendations to application & tooling upgrades, improvements & end of support/life replacements that will or may impact application operation, performance and support.
- Review Delivery team development artefacts and supporting documentation for each Release Candidate to prepare for deployment and support in Production.
- Provide support to the deployment and testing of approved application and application support tools in Production environments. Provide advice and assistance as required to other operational teams. This includes delivery of associated automated applications and testing as required.
- Support testing activities and advise development teams on acceptance into service criteria including NFRs and code quality targets.
- Identify, document and undertake application and database level monitoring, checking and routine maintenance on applications and application tooling in accordance with vendor, Delivery team and industry best practice. Automation is to be used as a standard approach where feasible.
- Working in close collaboration with Environment Automation, 3<sup>rd</sup> Line and PET teams, support automated application releases to the Production environments in accordance with approved Release Notes and supporting documentation. Record release steps including identification of all errors, discrepancies or identified improvements then work with Service Transition and Delivery teams to incorporate into future releases.
- Deployment activities to include all relevant pre-deployment and post-deployment testing.
- Adopt and adhere to strict DTS change controls to ensure the baseline version control of the Production environments are maintained, all work must have an associated task in the authorised ServiceNow. Investigate and report on all discrepancies identified, agreeing and obtaining approval for all responses and corrective action (this can be retrospective if required to preserve and maintain live services; but must be justified).
- Document, acquire, test, plan, schedule, obtain change approval and deploy Production and Management layer application and application tooling security patching in accordance with MoJ and Operational Services technical and security advice and business requirements.
- Respond to incidents and alerts, recording all Root Cause Analysis and response actions in ServiceNow, ensuring that the appropriate Business Service availability is maintained. For Priority 1 incidents, investigations and remediation is to continue through to resolution.
- Investigate, conduct root cause analysis and make recommendations for identified problems, ensuring all activities and communications are updated on the Problem record. Work with 3<sup>rd</sup> line support teams to deploy fixes (including any hotfixes as appropriate).
- Provide proactive ongoing assessment of application and infrastructure monitoring tools trends to optimise performance through amending triggers, thresholds and health indicators
- Maintain the technical Knowledge Base to document lessons learnt and routine tasks.
- Provide information, advice for and participate in retrospectives and Post Implementation Reviews as required.
- Provide weekly and ad hoc service reports on application performance, service incidents, problems and business usage.
- Provide information, documentation, knowledge transfer, handover and training to HMCTS Digital and Technology Services (DTS) team members as and when agreed.
- Support Optimisation activities required by the supported Services.
- Fulfil requests to provide anonymised data from Production Environments of the supported Services

## Scope of Environment Support by Service

The following table illustrates which environments need to be supported by this contract.

Service	Non-Live Environments				Live Environments		
	STE	DEV	SIT	NFT	PRP	PRD	BAE
<b>Common Platform</b>	Not in Scope	Not in Scope	Not in Scope	Not in Scope	In Scope	In Scope	In Scope
<b>IDAM</b>	Not in Scope	Not in Scope	Not in Scope	Not in Scope	In Scope	In Scope	In Scope
<b>ROTA</b>	Not in Scope	Not in Scope	Not in Scope	Not in Scope	In Scope	In Scope	N/A
<b>Atlassian</b>	Not in Scope	Not in Scope	Not in Scope	Not in Scope	In Scope	In Scope	N/A

Additional notes:

- In scope covers both IaaS and PaaS components required to run the associated Services.
- Perimeter devices and components (for example, firewalls) are in scope for all Non-Live and Live environments.
- At contract commencement, only the SIT, PRD and BAE environments have external connectivity. The provisioning, management and support of the additional perimeter devices and components will be in scope for this contract.
- Management layer components (for example, Jenkins, Gerrit, Artefactory, Networks, Security components) are in scope for all Non-Live and Live environments.
- The addition of a parallel production environment for Common Platform will also be in scope when provisioned.

## Service Elements and Requirements

Service element	Requirement
<b>Operational Management Services</b>	<ul style="list-style-type: none"> <li>• Management services to lead the delivery of all Services in scope/mentioned in this document.</li> </ul>
<b>Production Services &amp; Development Support</b>	<ul style="list-style-type: none"> <li>• Application Support Services (See section 6 below)</li> <li>• Infrastructure Support and Environment Automation</li> </ul>
<b>Production Releases</b>	<ul style="list-style-type: none"> <li>• Deliver 2 releases per week, as required by the Programme delivery plan. One minor (weekday evening) and one major (weekend (Sat &amp; Sun)). This applies to all in scope Services.</li> <li>• Each release should be delivered into Pre-Production, Business Assurance Environment and Production.</li> </ul>
<b>Support Hours</b>	<ul style="list-style-type: none"> <li>• Monday to Saturday: 08:00 – 20:00</li> </ul>
<b>On Call/Out of Hours</b>	<ul style="list-style-type: none"> <li>• Monday - Saturday 20:00 - 08:00</li> <li>• Sunday 24 hours.</li> </ul>

### Scope of helpdesk support by Service

The following table details the Services and level of support required under this contract. Where support is not in scope, the Supplier is still required to work closely with other DTS and PET teams to deliver a seamless support service to the end users. Day to day collaboration at every level with all teams is required to ensure services are well maintained, supported and that changes/releases are delivered successfully.

Service	1 <sup>st</sup> Line Sup'	2 <sup>nd</sup> Line Sup'	3 <sup>rd</sup> Line Sup'	Live Infrastructure Sup'
Common Platform	Not in Scope	In Scope	Not in Scope	In Scope
IDAM	Not in Scope	In Scope	Not in Scope	In Scope
ROTA	Not in Scope	In Scope	Not in Scope	In Scope
Atlassian	Not in Scope	Not in Scope	Infra Only	In Scope

### Other Services

- Project management for delivery of Services under this Calloff Contract – change management, project management, service management, release approvals, release automation in conjunction with DTS Operational teams
- Encourage closer and collaborative working across all technical and non-technical stakeholders
- Knowledge Transfer - Providing knowledge and skills transfer to HMCTS nominated members, or their representatives, during transition to future operations.



## Key Performance Indicators (KPI)

This table describes the KPIs and associated measurement techniques which the Supplier agrees to meet for this service.

KPI no	Target	Measurement	Measured by	Applies to:
1	Communication: To provide a full service during the agreed project. This includes agreed working hours and out of hours on call support of business-critical services.	The Supplier is to answer calls and respond to notifications or alerts within a timely manner. To ensure queries are responded to within the time laid out below.	To be reviewed within Supplier Relationship Management Meeting.	All
1a	P1 Incidents.	Respond to within 15 minute Service Level Target (SLT). *	100% ServiceNow report.	Live Support
1c	P2 Incidents.	Respond to within 30 minute Service Level Target (SLT). *	100% ServiceNow report.	Live Support
1e	P3 Incidents.	Respond to within 60 minute Service Level Target (SLT). *	100% ServiceNow report.	Live Support
1g	P4 Incidents.	Respond to within 120 minute Service Level Target (SLT). *	100% ServiceNow report.	Live Support
2	Availability and Delivery: Supplier is to ensure availability of all resources required to deliver each module of this agreement.	Live support must have a support presence available throughout core support hours 08:00 to 20:00 Monday to Saturday less Public Holidays unless formally agreed by the authority.	If Supplier is not able to complete planned work on a stated day they must obtain agreement from the relevant Product or Service Manager of alternate date.	Live Support
2a	To successfully release deployments and changes into Pre-Production environments.	Deployments have been conducted successfully in accordance with Release Note and plans within the agreed window.	95% Post Implementation Review.	Live Support
2b	To successfully release deployments and changes into Production environments. This includes the parallel Production environment when provisioned.	Deployments have been conducted successfully in accordance with release note and plans within the agreed window.	95% Post Implementation Review.	Live Support

KPI no	Target	Measurement	Measured by	Applies to:
2c	To successfully release deployments and changes into Business Assurance environments.	Deployments have been conducted successfully in accordance with release note and plans within the agreed window.	95% Post Implementation Review.	Live Support
2d	P1 Major Incidents that are within the control of the Live Services Team.	Target Resolution/Escalation within 4 hour	90% ServiceNow report.	Live Support
2e	P1 Incidents that are within the control of the Live Services Team.	Target Resolution/Escalation within 6 hours	100% ServiceNow report.	Live Support
2f	P2 Incidents that are within the control of the Live Services Team.	Target Resolution/Escalation within 8 hours	90% ServiceNow report.	Live Support
2g	P3 Incidents that are within the control of the Live Services Team.	Target Resolution/Escalation within 12 hours	90% ServiceNow report.	Live Support
2h	P4 Incidents that are within the control of the Live Services Team.	Target Resolution/Escalation within 21 hours	90% ServiceNow report.	Live Support
3	Quality: All elements of the service are fit for purpose. Meetings are conducted in a professional manner and uphold the standard of the Customers expectation.	Review of feedback to be provided from the departmental customer, internal stakeholders and the Service Manager.	95%	All
3a	Supplier is to ensure that all changes made in the Live environment (Pre-Production, Business Assurance and Production) are authorised.	Ensure that all changes are managed and recorded in the ServiceNow tool, with the required approval granted prior to conducting any work.	100%	Live Support
3b	Supplier is to ensure that all staff comply to security, data and information handling policies.	Breaches will be reported to and recorded by operational security.	No major and less than 3 minor incidents per calendar month. Repeated occurrences may result in termination of this contract.	All
3c	Supplier is to ensure that all staff adhere to the Operational Security Guide and Use of Personal Laptops Guide.	Breaches will be reported to and recorded by operational security.	No major and less than 3 minor incidents per calendar month. Repeated occurrences may result	All

KPI no	Target	Measurement	Measured by	Applies to:
	Production (LIVE) services must only be accessed via secure Laptops that meet NCSC requirements.		in termination of this contract.	
4	Invoice Accuracy: The Supplier will ensure that no invoice is supplied without the correct information as outlined with the Order Form of this Call-Off agreement; eliminating any invoice queries for the departmental customer.	Ensure a valid purchase order number is quoted on every invoice and that approval is sought from the departmental customer.	95% All invoices without a valid purchase order number will be put into query and therefore payment delayed or potentially not made on time.	
5	Management Information: To be supplied to CCS no later than the 7th of each month without fail. Reports are to be submitted via MISO.	CCS Review.	100% Failure to submit will fall in line with FA KPI.	
6	The resolution of Problem velocity is to be measured against the priority target level to ensure strong progress is achieved against the service backlog.	Monthly review of open Problems assigned to each Module in ServiceNow against agreed target resolution date.	95% Each open Problem must have the priority and target resolution agreed with the DTS Problem Manager	
7	Stage Gate Reviews The supplier's resources will assist with the work necessary to achieve clean passage through internal Programme Gates as well as any external Gates required – e.g. those prescribed by the GDS Service Manual.	Output / scorecard from Gate Review process.	Target is 100% through staged gates.	

The Buyer and Supplier will work together to review and continuously improve the SLAs and KPIs for the Services being delivered under this Call-Off Contract.

## Service Performance Measures

To deliver this service the Supplier must be able to provide the following requirements:

Performance Criteria	Key Indicator	Performance Measure
Expertise in cloud services, specifically Azure and all infrastructure elements associated with the products.	Weekly environment meeting	The supplier can evidence ITSM/Jira tickets/ emails confirming that issues are being progressed
Ability to provision, enhance and support a full Continuous Integration/ Continuous Deployment (CI/CD) infrastructure strategy utilising best practice and tooling in line with HMCTS guidelines	Monthly release statistics	HMCTS assurance targets are consistently achieved and Jira tickets against individual team pipelines are not trending an increase
Provision of technical services for Crime services transitioned into DTS, in line with standards set by HMCTS	Consistent approach towards development/ deployment and clear documentation	Acceptance by DTS operations via the Platform Compliance Authority
Delivery of technical services to undertake tech spikes and proofs of concept for the cross-cutting functions of HMCTS against the requirements of the HMCTS programmes	Clear documented outcomes of spike	Evidence of planned approach and execution with actionable recommendations
Evangelising industry best practices (complimenting HMCTS standards) to define standards within the applications development teams, and aid enforcement of compliance to HMCTS/GDS standards	Escalation to PCA or TDA for solutions that do not fit with current or future strategy  Ongoing input into what the future strategy looks like based on emerging technological trends	Working with the Platform Compliance Authority on latest best practice
Ongoing adherence to the HMCTS	Platform Compliance	Supplier can demonstrate

Cloud Governance Framework supporting convergence to, and compliance with, Reform Programme best practice.	Authority	deliverables against HMCTS Cloud road map monthly
Delivery of a backup strategy for new applications being deployed including retention periods and restoration as agreed by HMCTS central architecture	Documented process with testing  Clearly documented Recovery Point Objectives and Recovery Time Objectives	Supplier can show real-time back up process and proof of DR/ BCP restoration at the Buyer's request
Working with existing applications already deployed in infrastructure to define and deploy a back up strategy per the strategy for all new applications	Documented process with testing  Clearly documented Recovery Point Objectives and Recovery Time Objectives	Supplier can show real-time back up process and proof of DR/ BCP restoration at the Buyer's request
Delivery of cloud asset management across the cloud estate and ensuring compliance checks are performed and in place.	FinOps expectations  Security expectations	Supplier should be fully aware of all cloud infra and proactively aware of changes in line with PCA policy on a real-time basis
All technical capabilities are to be aligned with the technical architecture specified by the HMCTS Technical Architecture Board.	Technical Design Authority (TDA)  Platform Compliance Authority (PCA)	Supplier can prove decisions on technologies are all approved by TDA/ PCA prior to build and implementation
<u>Maintain business services and continuity</u>		
The ability to ensure that knowledge is developed, maintained and retained in order to maintain a good quality Service to the HMCTS during the term of the contract and in order to fulfil and meet the demands of HMCTS across Work Orders/SOW with no impact to HMCTS.	Knowledge management	Service up time is maintained per SLA's  Incident resolution is maintained per SLA's

HMCTS will have key milestones and commitments set both internally and externally by stakeholders; having reviewed and agreed milestones that are achievable should be met by suppliers	Meeting schedule / plan	Defined schedule / plan agreed with confirmed milestones and metrics  Supplier met milestones and metrics as defined in the schedule / plan
There is clear contract management reporting provided which covers delivery and commercial management reports and meetings	Reporting	Delivery  Financial  Onboarding / service provision health check  Partnering behaviours
The team should be able to understand the wider context of the services they are supporting; they are not simply transactions but services that have an impact on users lives.  The service provider should seek to understand the context that the services operate in and the users they serve.	Team knowledge on client products and process	Is the team knowledgeable about HMCTS and its services?  Does the team understand the wider landscape that HMCTS has to interact with?  Does the team understand the impact on users
Communications about how the service is performing, anything that is impacting or likely to impact the service as well as any resolutions are important for users, stakeholders and partners. These should be clear and provided regularly so that all parties are informed  Additionally, suppliers should provide clear communications about all of the services they are supporting; this should be in respect of the relationship between the supplier and HMCTS	Communications	Are communications clear and easy to follow for service users  Communications are done in a timely manner

<p>Planning for knowledge transfer/handover, transition into Live Operations with DTS and continued support of the service (including any revisions, updates and changes that need to be implemented) should be clearly planned, impacts and risks understood and delivered in a measured and careful manner utilising quality standard.</p>	<p>Planning and Delivery</p>	<p>Number of unresolved issues</p> <p>Current resource allocation</p> <p>Actual vs Estimated effort</p> <p>Actual vs Estimated resources</p> <p>Actual vs Estimated spend</p> <p>Backlog of work</p> <p>% increase / decrease of backlog</p> <p>Issues found in code review</p> <p>Issues found by QA</p> <p>Issues found by customers</p>
<p>Suppliers should adhere to a clearly defined change management process for all aspects of work. The centrally agreed change management framework for live services (as defined by HMCTS DTS) should be adhered to, and changes clearly documented as part of the process.</p>	<p><i>Change Management</i></p>	<p>Number of change requests (that are not initiated because of a Business change) within project scope:</p> <ul style="list-style-type: none"> <li>• on project milestones</li> <li>• after deployment</li> </ul> <p>Number of defects on requirements bugs</p>
<p>Suppliers will be measured on the effectiveness of Live Operational service implementations in terms of knowledge transfer, transition into Live operational status, ownership of live services. This should be done in the context of being proportionate and measured; delivered and supported services need to be offering continued value.</p>	<p><i>Effectiveness</i></p>	<p>Contribution - Value of benefits brought in with changes.</p> <p>Any innovations implemented?</p> <p>Ability to manage budget and needs? (<i>avoid Gold Plating</i>)</p> <p>Velocity of execution</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 clause 8.3 of the Framework Agreement.

## **2. Background to the agreement**

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.



<b>Signed</b>	Supplier	Buyer
<b>Name</b>	REDACTED	REDACTED
<b>Title</b>		
<b>Signature</b>		
<b>Date</b>	[	

## Schedule 1: Services

The Supplier will deliver to the Buyer Live Services Support and Production Management Services as detailed in:

- The Supplier's GCloud 12 Service Offering Reference 875602076621030 - Cloud Engineering and Support
- The Buyers Requirements document entitled "Crime Live Services Support and Production Management - Requirements vFINAL"



Crime Live Services  
Support and Producti

- The Supplier's Response to the Buyer's Requirements entitled "Method BDT – Crime Live Services Support and Production Support Clarifications"



Methods BDT - Crime  
Live Services Support

## Schedule 2: Call-Off Contract charges

**Call-Off Contract Charges:** The Buyer and Supplier have agreed the pricing mechanism for the core Live Services Support and Production Management Services under this Call\_Off Contract shall be a Fixed Monthly charge as detailed in Table 1 below. The Buyer and Supplier may choose to enter into additional Work Packages for additional Services which are not included within the core Live Services Support and Production Management Services Fixed Charge. For the Services, the applicable Call-Off Contract Charges 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:

**Table 1: Monthly service charge**

Service	Charge in £
Fixed Monthly Charge for Live Services Support and Production Management	REDACTED

**Rate card for workpackages**

Work packages for additional Services will only be agreed if the Buyer agrees that those additional Services sit outside of the core Services covered within the scope of the requirements outlined in Schedule 1. The Buyer and Supplier shall agree during the development of any Work package the most appropriate pricing mechanism for that Work Package which may include Time and Materials, Capped Time and materials, Fixed Price or any other agreed pricing mechanism.

The following Table 2 states the maximum Daily Rates agreed by the Buyer and Supplier which shall apply to the calculation of all Work Packages. Daily Rates are exclusive of VAT and include expenses within the M25.

**Table 2**

Role description	SFIA Staff Grade	Day Rate in £
Service Delivery Lead (also Release Manager)	6	REDACTED
Technical Delivery Lead (unbilled, accounted for in Non-Live costs)	6	REDACTED
Scrum Master (unbilled, value-add admin/reporting, cost absorbed)	3	REDACTED
AMS Tech Lead	5	REDACTED
EMS Tech Lead (oversight Live and Non-Live)	5	REDACTED
AMS Engineer	5	REDACTED
DevOps Engineer (blend Live and Non-Live according to programme priority)	5	REDACTED
AMS engineer	4	REDACTED
EMS engineer (blend Live and Non-Live according to programme priority)	4	REDACTED
DBA	4	REDACTED
Technical Architect	5	REDACTED

## Part B: Terms and conditions

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

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

### 2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)

- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

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

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

### 3. Supply of services

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

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

### 4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 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 its own due diligence

## 6. Business continuity and disaster recovery

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

## 7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

## **9. Insurance**

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.
- 9.2 The Supplier will ensure that:

- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
- 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- 9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
  - 9.4.1 a broker's verification of insurance
  - 9.4.2 receipts for the insurance premium
  - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
  - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
  - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
  - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
  - 9.8.1 premiums, which it will pay promptly
  - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

## 10. Confidentiality

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

## 11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- 11.5.1 rights granted to the Buyer under this Call-Off Contract
  - 11.5.2 Supplier's performance of the Services
  - 11.5.3 use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
- 11.6.1 modify the relevant part of the Services without reducing its functionality or performance
  - 11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - 11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.7 Clause 11.5 will not apply if the IPR Claim is from:
- 11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.7.3 other material provided by the Buyer necessary for the Services



- 11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the 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.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets:  
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
  - 13.6.3 the National Cyber Security Centre's (NCSC) information risk 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/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15. Open source

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

## 16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use 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 (and the Buyer of any Buyer Confidential Information breach). 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 is reasonable compensation and covers all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- 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); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
    - 8.44 to 8.50 (Conflicts of interest and ethical walls)

- 8.89 to 8.90 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

## 20. Notices

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

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

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

## 21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
  - 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
  - 21.6.2 there will be no adverse impact on service continuity
  - 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
  - 21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
  - 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
  - 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
  - 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

## **22. Handover to replacement supplier**

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

## **23. Force majeure**

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

## **24. Liability**

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

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

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

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common



law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

## **25. Premises**

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

## **26. Equipment**

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

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

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

## 28. Environmental requirements

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

## 29. The Employment Regulations (TUPE)

- 29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.
- 29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:
  - 29.2.1 the activities they perform
  - 29.2.2 age
  - 29.2.3 start date
  - 29.2.4 place of work
  - 29.2.5 notice period
  - 29.2.6 redundancy payment entitlement
  - 29.2.7 salary, benefits and pension entitlements
  - 29.2.8 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
- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause

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

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

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

### 30. Additional G-Cloud services

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

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

### 31. Collaboration

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

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

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

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

### 32. Variation process

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

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

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

### 33. Data Protection Legislation (GDPR)

- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement

Not Used

## Schedule 4: Alternative clauses

Not Used

Schedule 5: Guarantee

Not Used

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>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</li> <li>created by the Party independently of this Call-Off Contract, or</li> </ul> <p>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.</p>
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.
<b>Buyer Software</b>	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.



<b>Call-Off Contract</b>	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.
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	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.
<b>Commercially Sensitive Information</b>	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.
<b>Confidential Information</b>	Data, Personal Data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> <li>• 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</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the GDPR.
<b>Crown</b>	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.
<b>Data Loss Event</b>	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.

<b>Data Protection Legislation (DPL)</b>	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws 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 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
<b>Data Subject</b>	Takes the meaning given in the GDPR
<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• 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</li> </ul> <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>
<b>Deliverable(s)</b>	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
<b>Digital Marketplace</b>	The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	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.
<b>Equipment</b>	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.

<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	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: <a href="https://www.gov.uk/guidance/check-employment-status-for-tax">https://www.gov.uk/guidance/check-employment-status-for-tax</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.
<b>Force Majeure</b>	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• 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</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• 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</li> </ul>
<b>Former Supplier</b>	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 Sub-contractor or the Supplier (or any subcontractor of the Subcontractor).
<b>Framework Agreement</b>	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
<b>Fraud</b>	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.

<b>Freedom of Information Act or FoIA</b>	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.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
<b>GDPR</b>	General Data Protection Regulation (Regulation (EU) 2016/679)
<b>Good Industry Practice</b>	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.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	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.
<b>Implementation Plan</b>	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.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
<b>Insolvency event</b>	Can be: <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> </ul>

	<ul style="list-style-type: none"> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> </ul>
<b>Intellectual Property Rights or IPR</b>	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>
<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	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.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
<b>Law</b>	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>LED</b>	Law Enforcement Directive (EU) 2016/680.

<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	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.
<b>Management Charge</b>	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.
<b>Management Information</b>	The management information specified in Framework Agreement section 6 (What you report to CCS).
<b>Material Breach</b>	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.
<b>Ministry of Justice Code</b>	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.
<b>New Fair Deal</b>	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.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.
<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.

<b>Party</b>	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the GDPR.
<b>Processing</b>	Takes the meaning given in the GDPR.
<b>Processor</b>	Takes the meaning given in the GDPR.
<b>Prohibited act</b>	<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"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>
<b>Project Specific IPRs</b>	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.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	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.
<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government’s high-performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	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.

<b>Relevant person</b>	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.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	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.
<b>Replacement supplier</b>	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).
<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Digital Marketplace.
<b>Service Personal Data</b>	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.
<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	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.



<b>Subcontractor</b>	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.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.
<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier staff</b>	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.
<b>Supplier terms</b>	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.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

## Schedule 7: GDPR Information

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

### Annex 1: Processing Personal Data

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

- 1.1 The contact details of the Buyer's Data Protection Officer are: REDACTED
- 1.2 The contact details of the Supplier's Data Protection Officer are: REDACTED
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	<p><b>The Buyer is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"><li>• Personal data relating to defendants, prosecutors and any other party involved with a criminal case proceeding. Example of such data include: names, date of birth, addresses and current and/or previous convictions and offences.</li><li>• Personal data relating to HMCTS staff , including names, date of birth and their position within he organisation.</li></ul>
Duration of the Processing	For the duration of this contract
Nature and purposes of the Processing	This service provider will be handling the data for a sole purpose of managing and supporting

	the live services. The system and data will be accessed whilst carry out maintenance, debugging problems and troubleshooting issues with users.
Type of Personal Data	Name, address, date of birth, NI number, telephone number, pay, images, current and previous criminal convictions and offences and driver record details.
Categories of Data Subject	Staff (including, agents, and temporary workers), members of the public and users of the services.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The systems in scope for this services will be used to maintain historic records and sequence of events. Any data being processed should remain on the Buyers systems. Data should be destroyed in line with the Buyers standards and requirements, if requested