G-Cloud 13 Call-Off Contract

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

G-Cloud 13 Call-Off Contract

Part A: Order Form

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

G-Cloud 13 Call-Off Contract Order Form

Platform service ID number	[REDACTED]
Call-Off Contract reference	[REDACTED]
Call-Off Contract title	His Majesty's Courts and Tribunals Contact Center as a Service (CCaaS)
Call-Off Contract description	This Call-Off Contract involves the Supplier delivering a cloud-based Contact Center as a Service (CCaaS) solution, to the Buyer (His Majesty's Courts and Tribunals Service). The Supplier will manage the implementation, integration, and support of the system, ensuring it meets the Buyer's operational needs, security standards, and service level agreements. The solution seeks to enhance the Buyer's customer service capabilities across multiple communication channels.
Start date	31st October 2024
Expiry date	30th October 2027
Call-Off Contract value	[REDACTED]
Charging method	[REDACTED]

Purchase order number	TBC

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

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

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

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

From the Buyer	Secretary of State for Justice, on behalf of the Crown, Ministry of Justice, 102 Petty France, London, SW1H 9AJ
To the Supplier	Kerv Experience Limited 1 Finsbury Avenue, London, EC2M 2PF Company number: 03925996
Together the 'Parties'	

Principal contact details

For the Buyer:

[REDACTED]

For the Supplier:

[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **31st October 2024** and is valid for 36 months. Following a 6-month Ramp Period (as defined in Schedule 2) the Genesys Cloud subscription will start from the 1st May 2025.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of 60 days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier no less than 14 days written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. The Buyer hereby agrees any extensions which extend the Term beyond 36 months are only permitted subject to the Suppliers compliance with the additional exit plan requirements at clauses 21.3 to 21.8 of the Call Off Contract. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

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

<table>
<tr><td>G-Cloud Lot</td><td>[REDACTED]</td></tr>
<tr><td>G-Cloud Services required</td><td>The Services to be provided by the Supplier under the above Lot is listed in Framework Schedule 4 and outlined below:
Genesys Cloud CX
Genesys, Professional Services
Shelf Knowledge Management
Shelf Knowledge Management, Professional Services
PCI Pal
PCI Pal, Professional Services
Kerv CX Vizz and CX Email
Kerv Experience, Professional Services
Kerv Experience, Managed Service
Gamma, Voice Services</td></tr>
<tr><td>Additional Services</td><td>N/A</td></tr>
<tr><td>Location</td><td>[REDACTED]</td></tr>
<tr><td>Quality Standards</td><td><table><tr><th>#</th><th>Standard</th></tr><tr><td>1</td><td>MoJ Justice Digital Strategy as documented at: https://www.gov.uk/government/publications/ministry-of-justice-digital-strategy-2025</td></tr><tr><td>2</td><td>Buyer's Cyber Security Guidance - Technical User Edition as documented at: https://security-guidance.service.justice.gov.uk</td></tr></table></td></tr>
</table>

	3	Cloud guide for the public sector as documented at: *https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector*
	4	National Cyber Security Centre, Cloud Security guidance *https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles*
	5	NCSC Cyber Assessment Framework as documented at: *https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework*
	6	Technology Code of Practice as documented at: *https://www.gov.uk/guidance/the-technology-code-of-practice*
	7	Technology Code of Practice as documented at: *https://www.gov.uk/guidance/the-technology-code-of-practice*

<table>
<tr><td>Technical Standards:</td><td>
<table>
<tr><th>#</th><th>Standard</th></tr>
<tr><td>1</td><td>The World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA

Genesys Cloud is the primary User Interface for the Buyer’s users and administrators. Genesys Cloud is currently WCAG 2.1 AA compliant and is actively working towards WCAG 2.2 AA compliance by July 2025. Genesys will conduct 3rd party reviews 6 monthly to ensure WCAG adherence.</td></tr>
<tr><td>2</td><td>ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

Genesys Cloud is WCAG 2.1 AA compliant and is independently assessed.</td></tr>
<tr><td>3</td><td>ITIL V3</td></tr>
<tr><td>4</td><td>ISO/IEC 20000-1 2018 “Information technology — Service management – Part 1”

Buyer confirms alignment to this with a full certification road-mapped for FY 25/26.</td></tr>
<tr><td>5</td><td>ISO/IEC 20000-2 2019 “Information technology — Service management – Part 2”

Buyer confirms alignment to this with a full certification road-mapped for FY 25/26.</td></tr>
<tr><td>6</td><td>Payment Card Industry Data Security Standard (PCI DSS) as documented at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf</td></tr>
<tr><td>7</td><td>UK Government Baseline Personnel Security Standard https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</td></tr>
</table>
</td></tr>
<tr><td>Service level agreement:</td><td>Refer to Schedule 9 – Service Level Schedule.</td></tr>
</table>

Onboarding	[REDACTED]
Offboarding	[REDACTED]
Collaboration agreement	A formal collaboration agreement (as set out in Schedule 3 of the Call Off Contact terms) is not required and shall not apply. The Buyer and Supplier shall build an open, honest, and transparent working relationship. The relationship shall work as further set out in the '*Buyer specific amendments to/refinements of the Call Off Contract terms*' section below.
Limit on Parties' liability	[REDACTED]
Insurance	The Supplier insurance(s) required will be: • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. • This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure	A Party may end this Call-Off Contract if the other Party is affected by a Force Majeure Event that lasts for more than 20 consecutive days.
Buyer's responsibilities	The Buyer is responsible for ensuring:

	• co-operation with the Supplier in all matters relating to the Services; • provision (in a timely manner) of such information as the Supplier may reasonably request, and ensure that such information is accurate in all material respects; • it has all third party consents, licences and rights required in order to allow the Supplier and it's sub-contractors to provide the Services (at its own cost) preparation of the relevant premises and Buyer's equipment for the supply of the Services; and • the granting of access to relevant site/s. The Buyer shall use the Services in accordance with the terms of this Contract and any conditions notified in writing to the Buyer by the Supplier from time to time, for example any software licence terms. The Buyer shall ensure that the Services are not used: • for the transmission of any material which is intended as a hoax, for fraudulent purposes, or which is slanderous, offensive, abusive, obscene or of menacing nature or otherwise illegal; • by any third parties without the consent of the Buyer; and/or • in a manner which constitutes a violation or infringement of the rights of any person. The Services may include the archiving and retrieval of eligible communications made to and from the Buyer. The Services provide the Buyer with the ability to manage the retention period for recordings and access the recordings via Application Programming Interface (API) in order to retrieve and locally archive them. The Buyer must use the API to take all necessary backup copies of such recorded materials in order to meet its requirements and obligations. The retention periods for analytics, data and recordings are set out at https://help.mypurecloud.com/articles/retention-period-for-analytics-data-and-recording/. Accordingly, the Supplier shall not be liable for the loss of any recorded materials where the Buyer has failed to back up the same. If the Services include the provision of telephone lines and numbers, then in the event that the Buyer ceases to obtain such Services from the Supplier and migrates these Services to a third party, the Buyer shall ensure that any transfer or migration of Services or porting of telephone numbers is effected by such third party on the correct date. The Buyer

shall be responsible for any Charges that may apply when porting numbers away from the Supplier. The costs of such telephone lines and numbers shall remain payable by the Buyer to the Supplier for the remainder of the Call Off Term.

Prerequisites/Assumptions

The following Buyer responsibilities are hereby incorporated into this Call Off Contact:

- Buyer is responsible for all patch leads from switch port to phone.
- The Buyer is responsible for procuring and providing appropriate headsets.
- The Buyer will ensure that all user workstations meet the minimum system requirements for running the solution including WebRTC. The Buyer is responsible for general network and desktop troubleshooting and optimisation.
- Buyer is responsible for adding the Web Messenger snippet to the Buyer's website.
- Buyer to ensure that the network is ready prior to engineering site visit including any LAN-port configurations, DHCP, cable patching etc. for the new Services.
- Buyer will confirm there is space and dedicated power (number of power sockets etc.) for the equipment being installed at site and will arrange any remedial work ahead of planned install dates. Failure to comply could result in an aborted visit and Charges may apply to re-schedule.
- Any dual running costs (the cost of running the old and new networks in parallel) have not been included within these Contract commercials and will be the responsibility of the Buyer unless explicitly stated.
- Buyer will be accountable for ceasing any equipment, circuits and suppliers for their existing legacy network unless explicitly agreed otherwise with the Supplier.
- Buyer will facilitate attendance at site visits to ensure the Supplier will be guided to the correct locations.
- Buyer will ensure a nominated contact has authority to confirm the Supplier engineer has attended site. In the event that a sign off is required, the Buyer will ensure the appropriate personal are available.

	• Buyer is responsible for the internal communication of any agreed project schedule with their staff and relevant stakeholders. • Buyer will inform the Supplier of any Health & Safety risks prior to personnel attending site. • Buyer will assign a project manager ("**Buyer PM**"). Buyer PM will serve as a primary point of contact for Buyer with regards to the Solution and will be responsible for working closely with the Supplier team, including development of the project plan and for Buyer's internal coordination of resources to facilitate the Services to be performed by the Supplier hereunder. • Buyer will use reasonable endeavours to provide the Supplier with access to appropriate members of the Buyer's personnel, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Call Off Contract Period; • Buyer will provide sufficient and suitably qualified staff to fulfil the Buyer's roles and duties under this Call Off Contract as defined in the Implementation Plan; • Buyer will use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Call Off Contract provided that such documentation, data and/or information is available to the Buyer and is authorised for release by the Buyer.
Buyer's equipment	**[REDACTED]**

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Partners: • Genesys Europe BV. • Gemshelf Inc • PCI-PAL (U.K.) Limited • Gamma Telecom Holdings Limited

Call-Off Contract Charges and Payment

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

Payment method	[REDACTED]
Payment profile	[REDACTED]
Invoice details	[REDACTED]

Who and where to send invoices to	[REDACTED]
Invoice information required	All invoices submitted to the Buyer must clearly state the word 'invoice' and contain the following: • a unique identification number (invoice number) • company name, address and contact information • the name and address of the department/agency being invoiced • a clear description of what is being charged for • the date the goods or service were provided (supply date) • the date of the invoice • the amount(s) being charged • VAT amount if applicable • the total amount owed • A valid purchase order (PO) number
Invoice frequency	Invoice will be sent to the Buyer on an annual and monthly frequency, as set out within this Call Off Contract.
Call-Off Contract value	[REDACTED]
Call-Off Contract charges	[REDACTED]

Additional Buyer terms

Performance of the Service	This Call-Off Contract includes an implementation overview in Schedule 1: Services, and project milestones in the Payment Profile (Part A: Order Form). **[REDACTED]**
Guarantee	N/A
Warranties, representations	**[REDACTED]**
Supplemental requirements in addition to the Call-Off terms	**[REDACTED]**
Alternative clauses	These Alternative Clauses, which have been selected from Schedule 4, will apply: N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	The service specification covers the main deliverables, where further work is required, such will be covered by a change request. Throughout the lifetime of the project to implement the solution the Supplier will attend the Project Board in order to provide a progress update to the Project Board members. The Supplier acknowledges that the solution (set out in Schedule 1 of this Call Off Contract) is a component of the overall wider solution that is being implemented by the Buyer. Therefore, the Supplier will (acting reasonably) work collaboratively with the Buyer and the Buyer's other suppliers, where the Supplier is alerted to such and agrees same, as part of a delivery team within the established project structure and in accordance with the agreed required governance, to

	actively assist with the delivery of the solution and to ensure the solution within this Call Off Contract is delivered. For clarification the Supplier shall not be held accountable for any other supplier's deliverable save for working collaboratively with such supplier. Working collaboratively entails but is not limited to the following: · Contributing to the development and production of workstream delivery plans and the overall Buyer project plan; · Participating in activities to update and maintain workstream plans and the project plan; · Participating in the collective identification and management of workstream/project risks, issues and dependencies; · Attending and participating (as reasonably required) in working groups which will focus on specific aspects of project delivery, attendance at checkpoint and other governance meetings; · Contributing to the production of an approved end-to-end solution design; · Contributing to the preparation and execution of testing of the end-to-end solution; · Preparing for and executing the live implementation of the solution in line with Schedule 1 (whilst understanding Schedule 1 is one part of the wider solution being delivered to the Buyer). The Supplier agrees as part of the collective effort to reasonably prepare and deliver a transition to the new (wider) solution for all users and sites; · Compliance with the reasonable requirements that are established for the Buyer's acceptance of the solution into live service to ensure the solution is transitioned successfully to live service/BAU; · Allow the Buyer to engage directly with their sub-contractors who are involved in the delivery of the solution, where appropriate; · Extend these expectations (where applicable and appropriate) in relation to collaborative behaviour to their sub-contractors; · Participate in the service design activities associated with the production of the overall service wrap particularly in the development of the Supplier's OWA (Operational Working Agreement); · Work with the Buyer and other suppliers of the overall solution to resolve incidents and problems with the overall system.
Personal Data and Data Subjects	Schedule 7, Annex 1 shall apply to this Call Off Contract, as populated and appended below.

Intellectual Property	As per standard Call Off Terms
Social Value	[REDACTED]

1. Formation of contract

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

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

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

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

2. Background to the Agreement

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

Signed	Supplier	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]

Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Customer Benefits

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

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

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

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

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

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

2. Incorporation of terms

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

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)

- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

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

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

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

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

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

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

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

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

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

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

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

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

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

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

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

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

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

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

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

11.8.2 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

13.6.4 government best practice in the design and implementation of system components, including network principles, security design

principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

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

13.6.6 Buyer requirements in respect of AI ethical standards.

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

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

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will

reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

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

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

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

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

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

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

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

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

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including

conversion to open standards or other standards required by the Buyer

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

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

24. Liability

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

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

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

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

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

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

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29. 2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

29.5.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 1: Services

[REDACTED]

Schedule 2: Call-Off Contract charges

[REDACTED]

Schedule 3: Collaboration Agreement

N/A

Schedule 4: Alternative clauses

N/A

Schedule 5: Guarantee

N/A

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

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

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.

DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

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

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

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

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

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

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

Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.

Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.

Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

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

Annex 1: Processing Personal Data

[REDACTED]

Annex 2: Joint Controller Agreement

Annex 2: Joint Controller Agreement is N/A

Schedule 8 Buyer's Requirement Document

Functional Requirements

01 - Access Control

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-ACCMGNT-001	Access Management	Single Sign On	The supplier will ensure that the user only has to log in once to access all elements of the supplier's solution	Met	
CST-ACCMGNT-002	Access Management	Single Sign On	The supplier will ensure the solution can integrate with the buyers active directory via SAML 2.0 or other protocols supported by Azure AD for user authentication	Met	
CST-ACCMGNT-003	Access Management	Single Sign On	The supplier will ensure that Single Sign On can be used for user authentication with authorization being controlled by the solution	Met	
CST-ACCMGNT-004	Access Management	Single Sign On	The supplier will ensure that the solution can mix local authentication and single sign on access within a single instance of the Service	Met	
CST-ACCMGNT-005	Access Management	Location	The supplier will ensure that the solution can be accessed from any location defined by the buyer supporting direct access from homeworkers as well as staff at buyer's office locations.	Met	
CST-ACCMGNT-006	Access Management	Roles and privileges	The supplier will ensure that the Buyer can define sets of privileges and group these into roles.	Met	
CST-ACCMGNT-007	Access Management	Roles and privileges	The supplier will ensure that the Buyer can assign one or more roles to a user.	Met	
CST-ACCMGNT-008	Access Management	Roles and privileges	The supplier will ensure that a single user login can be used to perform admin, team leader and agent functions if granted the relevant roles and permissions.	Met	
CST-ACCMGNT-009	Access Management	Roles and privileges	The supplier will ensure that individual privileges can be assigned to a user.	Met	
CST-ACCMGNT-010	Access Management	Roles and privileges	The supplier will ensure the Buyer can control access to viewing reports and limit creation, editing and deletion of reports	Met	

CST-ACCMGNT-011	Access Management	User bulk import	The supplier will ensure that the Buyer can bulk import users via a CSV file.	Met	
CST-ACCMGNT-012	Access Management	Groups or teams	The supplier will ensure that a user can be a member of multiple groups	Met	
CST-ACCMGNT-013	Administration	Configuration	The supplier will ensure that the buyer can configure the capabilities identified in other requirements (e.g. Telephony, Email, webchat, routing and queueing, agent desktop options, recording policies, QM, WFM etc).	Met	
CST-ACCMGNT-014	Administration	Configuration	The supplier will ensure that the buyer can create and delete users (joiners and leavers), assign roles, permissions, allocate queues, skills etc.	Met	
CST-ACCMGNT-015	Access Management	Change ACD state	The supplier will ensure that designated users can change the ACD state of an agent	Met	
CST-ACCMGNT-016	Access Management	Change ACD state	The supplier will ensure that designated users can force logout an agent	Met	
CST-ACCMGNT-017	Access Management	Change ACD state	The supplier will ensure that if an agent has one or more contacts active when a force logout is performed, the contact(s) are returned to the relevant queue.	Partially met	Supervisors can force logout agents and Emails will return to the queue. Web Messaging (chat) is currently on the roadmap to also support the ability to return to open interactions in the queue when an agent is force logged out. Voice interactions cannot return to the queue if the agent is force logged out. Once an agent accepts a call, the call is "owned" by that agent until the call is completed. A forced logout interrupts the call flow, making it difficult for the system to automatically return the call to the queue.
CST-ACCMGNT-018	Access Management	Multiplicity and interruptibility	The supplier will ensure that the buyer can define multiplicity and interruptibility settings by group or agent.	Met	
CST-ACCMGNT-019	Access Management	Multiplicity and interruptibility	The supplier will ensure that the buyer can define the maximum number of simultaneous contacts per channel presented to an agent	Met	
CST-ACCMGNT-020	Access Management	Multiplicity and interruptibility	The supplier will ensure that the buyer can define whether one channel can interrupt another (e.g. If agent is working on an email, can this be interrupted by a voice call).	Met	

02 - Telephony

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-TEL-001	Telephony	Carrier Services	The supplier shall ensure that, if required, the solution can be integrated with a 3rd party Public Telephony (PSTN) access solution (I.e. Bring your own carrier)	Met	
CST-TEL-002	Telephony	Carrier Services	The supplier shall ensure the Carrier Services will not be impacted by the BT Openreach PSTN switch off	Met	
CST-TEL-003	Telephony	Carrier Services	The supplier shall port existing geographical numbers and non-geographical numbers as specified by the Buyer.	Met	
CST-TEL-004	Telephony	Carrier Services	The supplier shall allow designated users to amend the mapping of geographical numbers and non-geographical numbers as specified by the Buyer.	Met	
CST-TEL-005	Telephony	Carrier Services	The supplier shall provide reports of geographical numbers and non-geographical numbers used including allocated, unallocated and usage.	Met	
CST-TEL-006	Telephony	Carrier Services	The supplier shall provide geographical numbers and non-geographical numbers for use in the delivery of the Carrier Services (as and when requested by the Buyer).	Met	
CST-TEL-007	Telephony	Carrier Services	The supplier shall provide monthly billing data files providing a breakdown of telephony invoices.	Met	
CST-TEL-008	Telephony	Carrier Services	The supplier shall support the porting of geographical numbers and non-geographical numbers out of the Carrier Services to Other Suppliers.	Met	
CST-TEL-009	Telephony	Carrier Services	The supplier shall ensure that the Carrier Services are capable of integrating with other Carrier providers.	Met	
CST-TEL-010	Telephony	Carrier Services	The supplier will provide capabilities for the buyer to limit the phone number ranges that can be dialled by users (e.g. Bar access to premium rate numbers).	Met	
CST-TEL-011	Telephony	Call control	The supplier will ensure that the user can perform the following actions on telephony calls; dial a number, dial a contact in the directory, answer, hold, mute, transfer, conference, pause recording, resume recording, enter DTMF, hangup	Met	
CST-TEL-012	Telephony	Call control	The supplier will ensure that the user can conference up to 6 parties into a call.	Met	
CST-TEL-013	Telephony	Call control	The supplier will ensure that a user can conference both internal and external numbers into a call.	Met	
CST-TEL-014	Telephony	Call control	The supplier will ensure that a user can transfer a call to; an external number, a queue, another user as either a warm transfer or a cold transfer.	Met	

CST-TEL-015	Telephony	Call control	The supplier will ensure that a team leader can silently monitor an agent, coach (whisper to agent) or barge-in to the call.	Met	
CST-TEL-016	Telephony	Call control	The supplier will ensure that the Buyer is able to block calls from specific CLIs	Met	
CST-TEL-017	Telephony	Outbound voice	The supplier will provide capabilities to ensure that outbound calls will be associated with a queue. The user will be able to identify the queue associated with the outbound call.	Met	
CST-TEL-018	Telephony	Outbound voice	The supplier will ensure that a CLI can be configured against each queue and is used for outbound calls dialled from that queue.	Met	
CST-TEL-019	Telephony	Outbound voice	The supplier will ensure that the agent enters wrap up after an outbound call and is required to enter a wrap code for the call.	Met	
CST-TEL-020	Telephony	In queue callbacks	The supplier will ensure that the solution can offer customers the opportunity to retain their position in queue and be called back when their request is passed to an agent.	Met	
CST-TEL-021	Telephony	In queue callbacks	The supplier will ensure that the solution can capture a phone number if the customer wants to be called back on a different number.	Met	
CST-TEL-022	Telephony	In queue callbacks	The supplier will ensure that the buyer can limit the number of concurrent callbacks for a specific queue.	Met	
CST-TEL-023	Telephony	In queue callbacks	The supplier will ensure that the callback uses the DDI the customer rang as the CLI for the outbound call.	Met	
CST-TEL-024	Telephony	In queue callbacks	The supplier will ensure that the agent is presented with contact metadata, IVR menu choices etc when the callback is passed to the agent.	Met	
CST-TEL-025	Telephony	In queue callbacks	The supplier will ensure that the agent is engaged before the outbound call is dialled to remove any risk of a nuisance call.	Met	
CST-TEL-026	Telephony	In queue callbacks	The supplier will ensure that the agent is alerted that this is a callback, rather than an inbound call.	Met	
CST-TEL-027	Telephony	In queue callbacks	The supplier will ensure that the solution can be set to perform 1 callback only.	Met	
CST-TEL-028	Telephony	In queue callbacks	The supplier will ensure that the agent can send a SMS notification if the customer does not answer or is busy and the agent is unable to leave a voicemail.	Met	
CST-TEL-029	Telephony	Payments	The supplier will ensure that the solution is certified for PCI level 1 compliance to allow manual payments to be taken without depending upon a DTMF masking solution, payment IVR or other technology to descope PCI compliance from the contact centre solution.	Met	
CST-TEL-030	Telephony	Payments	The supplier will ensure that the agent can pause call recording when card information is provided by the customer.	Met	

CST-TEL-031	Telephony	Payments	The supplier will ensure that the agent can resume call recording when the customer has finished providing card information.	Met	

03 - Email

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-EML-001	Email	O365 integration	The supplier will ensure that the solution can integrate with the buyer's email servers.	Met	
CST-EML-002	Email	O365 integration	The supplier will ensure that customers only see and interact with the buyer's mailboxes.	Met	
CST-EML-003	Email	O365 integration	The supplier will ensure that outbound email appears to come from the buyer's mailboxes.	Met	
CST-EML-004	Email	Agent interface	The supplier will ensure that the agent is shown the from address, date received, title and body of the email.	Met	
CST-EML-005	Email	Agent interface	The supplier will ensure the agent can access the email thread if included in the body of the email.	Met	
CST-EML-006	Email	Agent interface	The supplier will ensure that the agent can open and read any attachments.	Met	
CST-EML-007	Email	Agent interface	The supplier will ensure that an agent can reply, reply all and forward the customer email.	Met	
CST-EML-008	Email	Agent interface	The supplier will ensure that an agent can send multiple outbound emails in response to a customer email.	Met	
CST-EML-009	Email	Agent interface	The supplier will ensure that an agent can download attachments included in a customer email.	Met	
CST-EML-010	Email	Agent interface	The supplier will ensure that CC and BCC destinations can be added to outbound email.	Met	
CST-EML-011	Email	Agent interface	The supplier will ensure that attachments can be added to an outbound email.	Met	
CST-EML-012	Email	Agent interface	The supplier will ensure that the agent can add a signature to outbound emails.	Met	
CST-EML-013	Email	Agent interface	The supplier will ensure that an agent can have different email signatures for different queues (relevant where agents work on different lines of business).	Met	
CST-EML-014	Email	Agent interface	The supplier will ensure that the agent can paste knowledge content into a draft email.	Met	
CST-EML-015	Email	Agent interface	The supplier will ensure that the agent can include URLs, images and forms (HTML content) into draft emails.	Met	

CST-EML-016	Email	Agent Interface	The supplier will ensure that the agent is able to view, access and pull emails queueing from the sender of the email the agent is processing	Met	
CST-EML-017	Email	Agent Interface	The supplier will ensure that the system can handle email attachments file sizes in line with O365 limits	Met	Currently (7th October 2024) 40MB in Genesys
CST-EML-018	Email	Agent Interface	The supplier will ensure that the email editor has rich text format (RTF) feature capabilities (e.g. italics, bold, underline, colour, font, text size, embedded images, bullets & numbering, indenting etc)	Met	
CST-EML-019	Email	Agent Interface	The supplier will ensure that the agent is able to defer and retrieve emails	Met	
CST-EML-020	Email	Email content retention	The supplier will ensure that the retention time for email content can be defined and the contents of email (inc attachments) older than retnetion time must be deleted. Note: This should not remove contact history, metadata and MI.	Met	
CST-EML-021	Email	Canned responses	The supplier will ensure that the agent can paste canned response content into draft emails.	Met	
CST-EML-022	Email	Canned responses	The supplier will ensure that the canned response templates can contain URLs, images, tables and other HTML content	Met	
CST-EML-023	Email	Storage	The supplier will ensure that a media library is available to support images, URLs	Met	

04 - Webchat

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-WEB-001	Webchat	Customer interface	The supplier will provide HTML/Javascript that can be deployed by the buyer into the buyer's websites	Met	
CST-WEB-002	Webchat	Customer interface	The supplier will provide a webchat client that can be passed parameters (e.g. website location, ID&V data etc).	Met	
CST-WEB-003	Webchat	Customer interface	The supplier will provide a webchat client that can be configured to meet Government Digital Service (GDS) presentation guidelines	Met	
CST-WEB-004	Webchat	Customer interface	The supplier will provide a webchat client that can be localised into Welsh	Met	
CST-WEB-005	Webchat	Customer interface	The supplier will provide a webchat client that allows the customer and agent to interact in Welsh	Met	
CST-WEB-006	Webchat	Customer interface	The supplier will provide a webchat client that can be hidden if there are no agents available	Met	

CST-WEB-007	Webchat	Customer interface	The supplier will provide a webchat client that can be hidden if the queue Estimated Wait Time (EWT) is above a configured threshold. The threshold should be configurable without changing the code deployed on to the website.	Met	
CST-WEB-008	Webchat	Customer interface	The supplier will provide a mechanism to collect data from the customer before the webchat is passed to the agent. This could be a pre-webchat form, automated interaction or other mechanism.	Met	
CST-WEB-009	Webchat	Customer interface	The supplier will ensure the webchat data collection capability allows, free text and defined options to be presented to the customer.	Met	
CST-WEB-010	Webchat	Customer interface	The supplier will ensure the webchat data collection capability free text entry will provide data format validation (e.g. email address formatting, case id format checking)	Met	
CST-WEB-011	Webchat	Customer interface	The supplier will ensure that data captured by webchat data collection will be presented to the agent when the contact is passed to the agent.	Met	
CST-WEB-012	Webchat	Customer interface	The supplier will ensure that data captured by webchat data collection will be available for use within contact routing rules	Met	
CST-WEB-013	Webchat	Customer interface	The supplier will provide a webchat client that presents comfort messaging whilst the webchat is queuing. The contents of comfort messaging will be defined within the contact routing rules.	Met	
CST-WEB-014	Webchat	Customer interface	The supplier will provide a webchat client that presents approximate Estimated Wait Time (EWT) remaining and/or position in queue at defined intervals as defined by contact routing rules.	Met	
CST-WEB-015	Webchat	Customer interface	The supplier will provide a webchat client that abandons the contact request if the webchat client is closed whilst the contact is waiting in queue.	Met	
CST-WEB-016	Webchat	Customer interface	The supplier will provide a webchat client that makes the customer aware when the agent is typing.	Met	
CST-WEB-017	Webchat	Customer interface	The supplier will provide a webchat client that allows the agent to post URLs, images and documents into the chat with this data being presented to the customer.	Met	
CST-WEB-018	Webchat	Customer interface	The supplier will provide a webchat client that allows the customer to request and be sent an email copy of the webchat transcript.	Met	
CST-WEB-019	Webchat	Customer interface	The supplier will provide a webchat client that allows the customer to opt in to a post webchat survey.	Met	
CST-WEB-020	Webchat	Customer interface	The supplier will ensure the Buyer is able to allow or restrict the usage of attachments in the webchat interface.	Met	

CST-WEB-021	Webchat	Customer interface	The supplier will ensure the buyer can download webchat transcripts	Met	
CST-WEB-022	Webchat	Webchat retention	The supplier will ensure that webchat transcripts are deleted based on business retention rules.	Met	
CST-WEB-023	Webchat	Co-browse (Screen share)	The supplier will provide a facility for screen sharing (co-browse) of the customer's desktop when permission is granted by the customer.	Met	

05 - Routing and Queuing

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-ROQU-001	Routing and Queueing	Routing all channels	The supplier will provide admin tools allowing the buyer to define the processing rules for routing voice, email, webchat contacts and tasks.	Met	
CST-ROQU-002	Routing and Queueing	Routing all channels	The supplier will ensure that routing configuration parameters can be defined outside the routing flow to allow designated users to adjust the routing rules without editing the routing flow.	Met	
CST-ROQU-003	Routing and Queueing	Routing all channels	The supplier will provide admin tools that allow the buyer to control the processing rules whilst a contact is queuing. Including but not limited to: a) Play announcements (voice) b) Play music (voice) c) Present comfort messaging (webchat) d) Inform customer of EWT and/or position in queue at intervals whilst queuing (webchat and voice) e) Change queue (e.g. if queue time has exceeded SLA) f) Change priority (e.g. if queue time has exceeded SLA)	Met	
CST-ROQU-004	Routing and Queueing	Routing all channels	The supplier will ensure that routing rules can call out to external APIs to perform business data lookup, additional analysis etc. The routing rules will take the response received and apply this to routing the contact.	Met	
CST-ROQU-005	Routing and Queueing	Routing all channels	The supplier will ensure that data collected during routing is saved as contact metadata for, routing decisions, presentation to the agent and for historical reporting.	Met	
CST-ROQU-006	Routing and Queueing	Routing all channels	The supplier will ensure the Buyer is able to create their own access points (for all channels - voice, email and webchat)	Met	
CST-ROQU-007	Routing and Queueing	Routing all channels	The supplier will ensure the Buyer is able revert back to a previous contact routing script/flow version	Met	
CST-ROQU-008	Routing and Queueing	Routing all channels	The supplier will ensure the Buyer is able to view the version history of contact routing script/flows	Met	

CST-ROQU-009	Routing and Queueing	Routing all channels	The supplier will ensure the Buyer is able to copy/clone contact routing scripts	Met	
CST-ROQU-010	Routing and Queueing	Routing all channels	The supplier will ensure the Buyer can configure routing rules to use agent proficiency for routing interactions	Met	
CST-ROQU-011	Routing and Queueing	Routing all channels	The supplier will ensure the system audits events (e.g. IVR changes, agent skills etc).	Met	
CST-ROQU-012	Routing and Queueing	Routing for voice	The supplier will ensure that open and close times can be configured per DDI with specific call flow sequence for out of hours calls.	Met	
CST-ROQU-013	Routing and Queueing	Routing for voice	The supplier will ensure that holidays (when Contact Centre is closed) can be configured per DDI.	Met	
CST-ROQU-014	Routing and Queueing	Routing for voice	The supplier will ensure that users can upload recorded announcements and include these in an IVR call flow	Met	
CST-ROQU-015	Routing and Queueing	Routing for voice	The supplier will ensure that prompts can be uploaded in .wav file format. (HMCTS currently uses Mono 64 bit.)	Met	
CST-ROQU-016	Routing and Queueing	Routing for voice	The supplier will ensure that the routing rules can include DTMF menus.	Met	
CST-ROQU-017	Routing and Queueing	Routing for voice	The supplier will ensure the Buyer can configure audio prompts to be either interruptible or uninterruptible	Met	
CST-ROQU-018	Routing and Queueing	Routing for voice	The supplier will ensure that the routing rules can include Text to Speech (TTS) announcements as well as pre-recorded voice announcements.	Met	
CST-ROQU-019	Routing and Queueing	Routing for voice	The supplier will ensure that the solution can provide Text to Speech (TTS) announcements.	Met	
CST-ROQU-020	Routing and Queueing	Routing for voice	The supplier will ensure that the IVR will provide UK English speech recognition (ASR).	Met	
CST-ROQU-021	Routing and Queueing	Routing for voice	The supplier will ensure that the routing rules enable customer data to be collected via DTMF	Met	
CST-ROQU-022	Routing and Queueing	Routing for voice	The supplier will ensure that data entry validation can be performed and customer re-entry requested if incorrect data is provided.	Met	
CST-ROQU-023	Routing and Queueing	Routing for voice	The supplier will ensure that global variable data can be captured from a call flow. For example, an emergency close line sets a global variable that is checked by all other voice call flows.	Met	
CST-ROQU-024	Routing and Queueing	Routing for voice	The supplier will ensure that multiple DDIs can be routed to the same queue.	Met	
CST-ROQU-025	Routing and Queueing	Routing for voice	The system will play a message and automatically cleardown queueing calls based on the number of agents logged in and time of day parameters.	Met	
CST-ROQU-026	Routing and Queueing	Routing for email	The supplier will ensure that routing can be defined based on the domain within the from address of the email received.	Met	

CST-ROQU-027	Routing and Queueing	Routing for email	The supplier will ensure that routing can be performed on keyword data extracted from the email title and body.	Met	
CST-ROQU-028	Routing and Queueing	Routing for email	The supplier will ensure that emails received into different mailboxes or having different keywords found in the content can be routed to the same queue	Met	
CST-ROQU-029	Routing and Queueing	Routing for email	The supplier will ensure that metadata can be identified and extracted from the email title/body content for use in routing (e.g. Find case id in customer email or SLA date in task notification email).	Met	
CST-ROQU-030	Routing and Queueing	Routing for email	The supplier will ensure that the routing for email can generate automatic customer responses (e.g. Thank you for your webform enquiry).	Met	
CST-ROQU-031	Routing and Queueing	Routing for webchat	The supplier will ensure the Buyer can create a sequence of automated exchanges to get additional data from the customer prior to passing the webchat to an agent.	Met	
CST-ROQU-032	Routing and Queueing	Routing for webchat	The supplier will ensure that the routing flow can analyse the customer data entry (e.g. Check that a case id entered is 16 digits, an email address contains an @ etc).	Met	
CST-ROQU-033	Routing and Queueing	Routing for webchat	The supplier will ensure that automated interactions can include pre-defined choices (e.g. opt in/out to post interaction survey).	Met	
CST-ROQU-034	Routing and Queueing	Routing for webchat	The supplier will ensure that all data captured from the customer will be saved for MI purposes and presented to the agent.	Met	
CST-ROQU-035	Routing and Queueing	Routing for tasks (if submitted via API rather than using email)	The supplier will ensure that routing can be performed on metadata included in the task request	Met	
CST-ROQU-036	Routing and Queueing	Routing for tasks (if submitted via API rather than using email)	The supplier will ensure that queuing rules can leverage task metadata (e.g. Change priority or queue if completion date is passed).	Met	
CST-ROQU-037	Routing and Queueing	Music	The supplier will ensure that royalty free music is available for use in queuing and hold scenarios.	Met	

06 - Agent Desktop

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-AGTDSK-001	Agent desktop	Softphone	The supplier will ensure that the agent desktop software is fully browser based and requires no desktop software installation	Met	
CST-AGTDSK-002	Agent desktop	Softphone	The supplier will ensure that the agent desktop can provide inbuilt softphone capability and no hardphone or Buyer's PBX is required.	Met	

CST-AGTDSK-003	Agent desktop	Redirect to landline/mobile	The supplier will ensure that telephony can be redirected to an agent's mobile, home number or office DDI if there is a bandwidth issue at the agent's location.	Met	
CST-AGTDSK-004	Agent desktop	Initial ACD state	The supplier will ensure that at login the agent will default to a not ready state.	Met	
CST-AGTDSK-005	Agent desktop	Directory	The supplier will ensure that agents can search a directory of users, groups or transfer numbers configured on the solution.	Met	
CST-AGTDSK-006	Agent desktop	Presence	The supplier will ensure the presence state of individuals will be shown for each user in the directory	Met	
CST-AGTDSK-007	Agent desktop	Outbound contact	The supplier will ensure that the agent can make an outbound call at any time when logged in.	Met	
CST-AGTDSK-008	Agent desktop	Outbound contact	The supplier will ensure that an agent can write and send an outbound email at any time when logged in.	Met	
CST-AGTDSK-009	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that manual and auto answer can be configured for agents.	Met	
CST-AGTDSK-010	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that when an agent is set as auto answer, contacts are automatically answered when presented to an agent.	Met	
CST-AGTDSK-011	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that when an agent is set to manual answer, contacts are requeued if not answered within the specified timeframe (RONA)	Met	
CST-AGTDSK-012	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the defined role can configure an audible warning and/or whisper when a contact is presented to an agent and automatically answered.	Met	
CST-AGTDSK-013	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that if an agent changes ACD state whilst handling a contact, the ACD state change is only applied when the agent finishes wrap up.	Met	
CST-AGTDSK-014	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the Buyer can configure, per queue, what contact metadata is presented to an agent	Met	
CST-AGTDSK-015	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the Buyer can define the layout and presentation of Contact metadata.	Met	
CST-AGTDSK-016	Agent desktop	Contact handling (voice, email, webchat)	The supplier will ensure that the presentation can include; CLI, number called, queue, IVR menu selection, IVR data entry (e.g. case id), email keyword analysis, webchat data capture, queue time, link to case record (based on case id identification), survey optin etc	Met	

CST-AGTDSK-017	Agent desktop	Contact handling (tasks)	The supplier will ensure that the presentation can include task details submitted via the task API request. E.g. Task type, due date, priority, task URL, task notes, case id etc.	Met	
CST-AGTDSK-018	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that contact metadata is available within Contact Detail Record MI for reporting purposes	Met	
CST-AGTDSK-019	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent can enter the case id associated with the contact.	Met	
CST-AGTDSK-020	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that contacts with professional users, allows multiple case ids to be captured for a single contact.	Met	
CST-AGTDSK-021	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent can capture notes about the contact for later reference.	Met	
CST-AGTDSK-022	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent is able to capture information about the customer (e.g. Name, email address, notes, case id, customer flags).	Met	
CST-AGTDSK-023	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the buyer can define what data fields are available to the agent for capturing customer data.	Met	
CST-AGTDSK-024	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that during repeat contacts, that the agent can see previously captured information about the customer.	Met	
CST-AGTDSK-025	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent can see previous interactions with the customer (on the same phone number or email address).	Met	
CST-AGTDSK-026	Agent desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent can access the detail of previous interactions, notes capured etc.	Met	
CST-AGTDSK-027	Agent Desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent is presented with relevant knowledge content for the contact being processed.	Met	
CST-AGTDSK-028	Agent Desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that the agent is presented with relevant knowledge content for the contact being processed and this is updated based on the content of the interaction, and updates as the interaction progresses.	Met	
CST-AGTDSK-029	Agent Desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that when an agent finishes a contact, that the agent is presented with wrap up reason codes specific to the queue.	Met	
CST-AGTDSK-030	Agent Desktop	Contact handling (voice, email, webchat and tasks)	The supplier will ensure that if configured the agent will be required to enter a wrap code before closing the contact.	Met	
CST-AGTDSK-031	Agent desktop	Multiplicity and interruptability	The supplier will ensure that a single agent UI is provided to handle voice, email, webchat and task interactions	Met	

CST-AGTDSK-032	Agent desktop	Blending	The supplier will ensure that agents can be delivered (pushed) the next contact from any channel (in any order) as defined by the queuing rules, agent skills etc.	Met	
CST-AGTDSK-033	Agent desktop	Multiplicity and interruptability	The supplier will ensure that agents can be allocated 1 or more concurrent contacts.	Met	
CST-AGTDSK-034	Agent desktop	Multiplicity and interruptability	The supplier will ensure that concurrency can be defined for the number of concurrent contacts by channel type	Met	
CST-AGTDSK-035	Agent desktop	Multiplicity and interruptability	The supplier will ensure that contacts (emails) can be extracted from a queue. This will not be limited by the multiplicity constraints. I.e. If an agent has multiplicity set to 2, and has 2 open emails, the agent can extract and pull an additional email from the queue.	Met	
CST-AGTDSK-036	Agent desktop	Multiplicity and interruptability	When an agent has multiple open contacts, the supplier will ensure that Average Handle time only increments for the "active" contact. (This is the contact that has focus on the agent desktop.)	Met	
CST-AGTDSK-037	Agent desktop	Multiplicity and interruptability	The supplier will ensure that the Buyer can define what work types can be interrupted by other work types.	Met	
CST-AGTDSK-038	Agent desktop	View schedule	The supplier will ensure that an agent can view their WFM schedule for the current and future days.	Note	Not available for this delivery as WEM tool being used by HMCTS is NICE IEX not Genesys
CST-AGTDSK-039	Agent desktop	Personal dashboard	The supplier will ensure that agents can see their personal performance by queue, including metrics such as AHT and contacts handled	Met	
CST-AGTDSK-040	Agent desktop	Personal dashboard	The supplier will ensure that agents can see their quality score by queue.	Met	
CST-AGTDSK-041	Agent desktop	Personal dashboard	The supplier will ensure that agents can see their customer survey score	Met	
CST-AGTDSK-042	Agent desktop	Personal dashboard	The supplier will ensure that agents can compare their performance against targets set, highlighting if the agent's performance metrics are outside the optimum range.	Met	
CST-AGTDSK-043	Agent desktop	Queue dashboard	The supplier will ensure that a dashboard is available to agents including queuing contact count for each of the queues that the agent is configured.	Met	
CST-AGTDSK-044	Agent desktop	Status	The supplier will ensure designated users can configure Not Ready Agent Statuses (Break, Lunch, Meeting, Training etc)	Met	

07 - RTS & MI

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-RTSMI-001	RTS & MI	Real time	The supplier will ensure that real time statistics (RTS) are presented for all worktypes (voice, email, webchat and tasks)	Met	
CST-RTSMI-002	RTS & MI	Real time	The supplier will ensure that real time statistics (RTS) can be displayed for each queue. Including but not limited to: a) The count of the contacts in the queue b) The age of the oldest in queue (may be multiple days old) c) AHT d) Abandonment rate e) Count of contacts processed today f) Count of callbacks queuing	Met	
CST-RTSMI-003	RTS & MI	Real time	The supplier will ensure that RTS dashboards can be created to display a subset of queues (e.g. for a specific Service)	Met	
CST-RTSMI-004	RTS & MI	Real time	The supplier will ensure that RTS dashboards can be deployed as wallboards.	Met	
CST-RTSMI-005	RTS & MI	Real time	The supplier will ensure that RTS can show the status of agents assigned to particular queues.	Met	
CST-RTSMI-006	RTS & MI	Real time	The supplier will ensure that the buyer can create custom RTS dashboards with tables, graphs and gauges for key contact metrics.	Met	
CST-RTSMI-007	RTS & MI	Real time	The supplier will ensure that RTS can display information on contacts in queue, allowing these to be searched for specific contacts.	Met	
CST-RTSMI-008	RTS & MI	Real time	The supplier will ensure that where a specific email contact is found in RTS, the contact can be pulled from the queue and delivered to the user.	Met	
CST-RTSMI-009	RTS & MI	Real time	The supplier will ensure that designated users can force cleardown of calls in queue or set of queues. (e.g. In an emergency outage scenario).	Met	
CST-RTSMI-010	RTS & MI	Historical	The supplier will ensure that historical statistics are presented for all worktypes (voice, email, webchat and tasks)	Met	
CST-RTSMI-011	RTS & MI	Historical	The supplier will ensure that historical data is captured from the point a contact is received by the CCaaS solution and is included in reports from that point. (A contact does not need to be completed or abandoned before it is being available for historical reporting.)	Met	
CST-RTSMI-012	RTS & MI	Historical	The supplier will ensure that reporting can be performed by agent and team, by queue and Service (group of queues), by channel and by date range.	Met	

CST-RTSMI-013	RTS & MI	Historical	The supplier will ensure that AHT is measured based on when a contact is active (has focus) on the agent desktop, not for the duration that the contact is open.	Met	
CST-RTSMI-014	RTS & MI	Historical	The supplier will ensure that talk, hold and wrap are captured as separate durations against the contact	Met	
CST-RTSMI-015	RTS & MI	Historical	The supplier will ensure that MI can report on callbacks, inbound and outbound calls separately.	Met	
CST-RTSMI-016	RTS & MI	Historical	The supplier will ensure that MI can be produced on outbound calls, including wrap time.	Met	
CST-RTSMI-017	RTS & MI	Historical	The supplier will ensure that reports can be produced comparing agent groups	Met	
CST-RTSMI-018	RTS & MI	Historical	The supplier will ensure that historical reports can be produced on contact information, quality data and customer survey data.	Met	
CST-RTSMI-019	RTS & MI	Historical	The supplier will ensure that historical data can be presented in tables and graphs.	Met	
CST-RTSMI-020	RTS & MI	Historical	The supplier will ensure that historical MI supports filtering based on report attributes (queues, teams, agents etc) and date/time ranges.	Met	
CST-RTSMI-021	RTS & MI	Historical	The supplier will ensure that historical MI supports the ordering of data within tables.	Met	
CST-RTSMI-022	RTS & MI	Historical	The supplier will ensure that historical MI supports the export of MI data in CSV format and the output of report presentation in PDF.	Met	
CST-RTSMI-023	RTS & MI	Historical	The supplier will ensure that APIs or MI data files will allow the buyer to extract MI data from the solution to feed into an external warehouse for advanced reporting activities.	Met	
CST-RTSMI-024	RTS & MI	Historical	The supplier will ensure that both summary data (15 minutes and daily) can be extracted as well as individual contact detail records	Met	
CST-RTSMI-025	RTS & MI	Historical	The supplier will ensure that when a CTSC user leaves (HMCTS), related MI data remains on the system	Met	
CST-RTSMI-026	RTS & MI	Historical	The supplier will ensure that MI users can report on all work types, and export to warehouse for reporting alongside contact data	Met	
CST-RTSMI-027	RTS & MI	Historical	The supplier will ensure that MI can be produced based on IVR options and wrap codes selected during a contact.	Met	
CST-RTSMI-028	RTS & MI	Historical	The Supplier will ensure Historical reports and MI data extract can include quality score data.	Met	

08 - Recording

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-REC-001	Recording	All channels	The supplier will ensure that the buyer can define which contacts are recorded, across all channels	Met	
CST-REC-002	Recording	All channels	The supplier will ensure that the buyer can define rules regarding which contacts should have screen recording enabled	Met	
CST-REC-003	Recording	All channels	The supplier will ensure that all screens are recorded (e.g. where an agent is using multiple screens).	Met	
CST-REC-004	Recording	Voice	The supplier will ensure that recording is paused when requested by the agent (e.g. taking manual payment)	Met	
CST-REC-005	Recording	Voice	The supplier will ensure that when voice recording is paused, that screen recording is also paused	Met	
CST-REC-006	Recording	Voice	The supplier will ensure that when trunk side voice recording is used, recording is paused whilst the customer is queuing or on hold.	Met	
CST-REC-007	Recording	Voice	The supplier will ensure that call recordings can be exported/downloaded as .wav files.	Met	
CST-REC-008	Recording	Voice	The supplier will ensure the buyer is able to configure permission to access call recordings	Met	
CST-REC-009	Recording	All channels	The supplier will ensure that contacts can be searched by queue, agent, date/time, contact metadata (e.g. case id), transcription keywords and speech categories	Met	
CST-REC-010	Recording	All channels	The supplier will ensure that contact details are presented alongside the call recording (and screen recording if present).	Met	
CST-REC-011	Recording	All channels	The supplier will ensure that recordings can be played via the web interface.	Met	
CST-REC-012	Recording	All channels	The supplier will ensure that playback supports pause, rewind, forward wind, go to specific point in call, go to start, go to end and annotation of the recording	Met	
CST-REC-013	Recording	All channels	The supplier will ensure that the buyer can define retention rules for recordings.	Met	
CST-REC-014	Recording	All channels	The supplier will ensure that recordings older than the retention time are deleted, however the metadata about the contact is retained for MI purposes.	Met	
CST-REC-015	Recording	All channels	The supplier will ensure that the buyer can lock specific recordings, with locked recordings being excluded from retention time deletion.	Met	
CST-REC-016	Recording	All channels	The supplier will ensure that all access to all recordings across all channels are logged for audit purposes	Met	

09 - Quality Management

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-QM-001	QM	Evaluation forms	The supplier will ensure that the buyer can design quality evaluation forms.	Met	
CST-QM-002	QM	Evaluation forms	The supplier will ensure that quality forms can be associated with relevant channels (voice, Email, webchat), services and queues.	Met	
CST-QM-003	QM	Evaluation forms	The supplier will ensure that evaluation forms can include radio button options, select lists and free text entry	Met	
CST-QM-004	QM	Evaluation forms	The supplier will ensure that answer options can be assigned a score.	Met	
CST-QM-005	QM	Evaluation forms	The supplier will ensure that answers can be set as pass/fail.	Met	
CST-QM-006	QM	Evaluation forms	The supplier will ensure that free text entry can be used by evaluators to explain the reason for a score.	Met	
CST-QM-007	QM	Evaluation forms	The supplier shall ensure the number of different evaluation forms that can be created is 50+	Met	
CST-QM-008	QM	Evaluation forms	The supplier will ensure the buyer can edit evaluation forms	Met	
CST-QM-009	QM	Evaluation forms	The supplier will ensure the buyer can configure scoring with different weightings per question	Met	
CST-QM-010	QM	Evaluation forms	The supplier will ensure that the buyer can save partial evaluations	Met	
CST-QM-011	QM	Evaluation forms	The supplier will ensure that designated users can delete evaluations	Met	
CST-QM-012	QM	Evaluation forms	The supplier will ensure free text boxes have a minimum limit of 3000 characters	Met	
CST-QM-013	QM	Evaluation forms	The supplier will ensure the buyer can configure that each evaluation question can contain a free text box and also configure a free text box for the overall evaluation.	Met	
CST-QM-014	QM	Evaluation forms	The supplier will ensure the evaluation form contains an inbuilt spell checker	Met	
CST-QM-015	QM	Evaluation forms	The supplier will ensure that the buyer can add hyperlinks in the free text box to allow quick access to additional information	Met	Not currently supported in evaluation forms but can be included in coaching and development
CST-QM-016	QM	Evaluation forms	The supplier will ensure that the system can auto save evaluations	Not met	Evaluations can be manually saved and can be saved as a draft or reassigned to another evaluator
CST-QM-017	QM	Access	The supplier will ensure that the buyer can define/permit who can delete drafts	Met	

CST-QM-018	QM	Assignment rules	The supplier will ensure that the buyer can define rules regarding the allocation of evaluations to evaluators	Met	
CST-QM-019	QM	Assignment RTS	The supplier will ensure that RTS are available identifying any failings to perform allocated evaluations	Met	
CST-QM-020	QM	Assignment alerts	The supplier will ensure that evaluators receive alerts to undertake the assigned evaluations.	Met	
CST-QM-021	QM	Feedback	The supplier will ensure that agents are able to receive feedback regarding evaluations performed.	Met	
CST-QM-022	QM	Search and Filtering	The supplier will ensure that the customer interactions can be searched or filtered on any content metadata	Met	
CST-QM-023	QM	Data	The supplier will ensure that the buyer can see agent related actions on the system during the interaction (e.g. wrap codes chosen, notes and flags).	Met	
CST-QM-024	QM	Data	The supplier will ensure that the buyer can see if an evaluation has been completed by someone else	Met	
CST-QM-025	QM	Email and Notifications	The supplier will ensure that the buyer can choose who to send completed evaluation to and share with	Met	
CST-QM-026	QM	Reporting	The supplier will ensure that MI can be produced for individual questions	Met	
CST-QM-027	QM	Reporting	The supplier will ensure that trend analysis can be performed for individual questions	Met	
CST-QM-028	QM	Reporting	The system will ensure the ability to change an evaluation form, whilst protecting historical data (e.g. if you delete a question from the evaluation form, you should still have sight of that question in the trend data)	Met	
CST-QM-029	QM	Speech & Text Analytics	The supplier will ensure that English voice calls can be automatically transcribed.	Met	
CST-QM-030	QM	Speech & Text Analytics	The supplier will ensure that Welsh voice calls can be automatically transcribed.	Not met	While Genesys Cloud does not currently support Welsh voice transcription, additional languages are always being added to Genesys Cloud.
CST-QM-031	QM	Speech & Text Analytics	Define rules for when transcription is enabled (e.g. what percentage of voice calls should be analysed or enable transcription for specific queues)	Met	
CST-QM-032	QM	Speech & Text Analytics	The supplier will ensure that email and chat text (excluding the contents of attachments) can be included in the analysis	Met	
CST-QM-033	QM	Speech & Text Analytics	The supplier will ensure the system can perform customer sentiment analysis based on keywords and phrases	Met	
CST-QM-034	QM	Speech & Text Analytics	The supplier will ensure the system can perform customer content analysis based on keywords and phrases	Met	

CST-QM-035	QM	Speech & Text Analytics	The supplier will ensure that searching for contacts based on sentiment tags is available.	Met	
CST-QM-036	QM	Speech & Text Analytics	The supplier will ensure that searching for contacts based on content tags is available.	Met	
CST-QM-037	QM	Speech & Text Analytics	The supplier will ensure the buyer can see the percentage of calls that are being transcribed	Met	
CST-QM-038	QM	Speech & Text Analytics	The supplier will ensure the buyer can improve and update transcription.	Met	
CST-QM-039	QM	Speech & Text Analytics	The supplier will ensure the buyer can export data (themes and associated MI) in CSV and/or Excel	Met	
CST-QM-040	QM	Speech & Text Analytics	The supplier will ensure the buyer can report trends and associated MI	Met	
CST-QM-041	QM	Speech & Text Analytics	The supplier will ensure the buyer can categorise calls and text into themes (based on keywords and phrases)	Met	
CST-QM-042	QM	Speech & Text Analytics	The supplier will ensure the buyer can differentiate between the customer and the agent handling the contact	Met	
CST-QM-043	QM	Speech & Text Analytics	The supplier will ensure the buyer can review telephony metrics and filter by themes/topics created by speech analytics	Met	
CST-QM-044	QM	Speech & Text Analytics	The supplier will ensure that real time notifications can be triggered based on audio content	Met	

10 - Surveys

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-SRVY-001	Surveys	Opt in	The supplier will ensure that customers have the ability to opt-in to be sent a survey	Met	
CST-SRVY-002	Surveys	Opt in	The supplier will ensure that surveys are only sent to customers that opt-in to taking a survey and then interacted with an Agent (e.g. Surveys are not to be sent to customers that opt-in for a survey but abandon in the queue before speaking to an agent).	Met	
CST-SRVY-003	Surveys	Survey invite	The supplier will ensure that customers can be sent a survey invite by email or SMS following a voice or webchat contact.	Met	
CST-SRVY-004	Surveys	Survey design	The supplier will ensure that the buyer can design surveys to meet Government Digital Service (GDS) presentation guidelines.	Met	
CST-SRVY-005	Surveys	Survey design	The supplier will ensure that surveys can contain multiple choice questions.	Met	
CST-SRVY-006	Surveys	Survey design	The supplier will ensure that surveys offer customers the opportunity to provide free text responses.	Met	

CST-SRVY-007	Surveys	Survey design	The supplier will ensure that survey questions can be scored.	Met	
CST-SRVY-008	Surveys	Survey design	The supplier will ensure that a customer can respond to multiple surveys	Met	
CST-SRVY-009	Surveys	Survey design	The supplier will ensure that the buyer can create a single survey that can be used for multiple queues and channels	Met	
CST-SRVY-010	Surveys	Survey Data	The supplier will ensure that survey data is retained for minimum 12mths	Met	
CST-SRVY-011	Surveys	Survey MI	The supplier will ensure that MI is captured for customers that both start and those that complete a survey.	Met	
CST-SRVY-012	Surveys	Survey MI	The supplier will ensure that survey data is linked to the contact so survey results can be attributed to the relevant date/time, agent, team, queue and Service - where the buyer has the ability to report on this data.	Met	
CST-SRVY-013	Surveys	Survey MI	The supplier will ensure that the buyer can identify survey completion rate	Met	
CST-SRVY-014	Surveys	Survey Reporting	The supplier will ensure the buyer can report on survey data from within the system	Met	
CST-SRVY-015	Surveys	Survey Reporting	The supplier will ensure that the buyer can access and export survey related data for reporting	Met	
CST-SRVY-016	Surveys	Survey Reporting	The supplier will ensure that survey reporting can combine survey data from different survey types.	Met	
CST-SRVY-017	Surveys	Survey Audit	The supplier will ensure that the buyer can view the survey version history	Met	

11 - Performance Management

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-PERFMGT-001	Performance Management	Metrics	The supplier will ensure that all metrics are available per agent, team, queue and channel	Met	
CST-PERFMGT-002	Performance Management	Metrics	The supplier will ensure that AHT, talk time, hold time and wrap time can be measured for all work types.	Met	
CST-PERFMGT-003	Performance Management	Metrics	AHT, talk time, hold time and wrap time is measured and presented independently for each channel (queue).	Met	
CST-PERFMGT-004	Performance Management	Metrics (Quality scores)	The supplier will ensure that completed QM evaluation result scores are available within performance management per agent, team, queue and channel	Met	

CST-PERFMGT-005	Performance Management	Metrics (Survey scores)	The supplier will ensure that survey result scores are available within performance management per agent, team, queue and channel	Met	
CST-PERFMGT-006	Performance Management	Metrics (Completed work)	The supplier will ensure that completed work counts are available within performance management per agent, team, queue and channel	Met	
CST-PERFMGT-007	Performance Management	Targets	The supplier will ensure that target ranges for good performance, acceptable performance and poor performance can be configured by the Buyer for each metric against each queue and channel	Met	
CST-PERFMGT-008	Performance Management	Agent dashboards	The supplier will ensure that agents can view their current performance and trend over time	Met	
CST-PERFMGT-009	Performance Management	Agent dashboards	The supplier will ensure that agents can compare their performance against targets set	Met	
CST-PERFMGT-010	Performance Management	MI	The supplier will ensure that MI can be produced measuring agent and team performance against targets	Met	
CST-PERFMGT-011	Performance Management	MI	The supplier will ensure that Team Leaders can view the performance of their team.	Met	
CST-PERFMGT-012	Performance Management	MI	The supplier will ensure that Team Leaders can compare performance to targets set.	Met	

12 - Knowledge Management

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partially met	Comments
CST-KM-001	Knowledge	Authoring	The supplier will ensure that the buyer can define article taxonomy.	Met	
CST-KM-002	Knowledge	Authoring	The supplier will ensure that the buyer can modify the taxonomy over time.	Met	
CST-KM-003	Knowledge	Authoring	The supplier will ensure that articles can include; URLs, HTML content, PDF, PNG, JPEG, GIF, word, excel, PowerPoint, Visio, mp3 and mp4	Met	
CST-KM-004	Knowledge	Authoring	The supplier will ensure that different versions of content are available to different user communities (e.g. Public/Internal).	Met	

CST-KM-005	Knowledge	Authoring	The supplier will ensure that access to specific articles can be limited to particular agent groups.	Met	
CST-KM-006	Knowledge	Authoring	The supplier will ensure that the solution identifies knowledge gaps	Met	
CST-KM-007	Knowledge	Authoring	The supplier will ensure that the solution can import or leverage content in external HTML documents	Met	
CST-KM-008	Knowledge	Authoring	The supplier will ensure that editing permissions can be constrained for particular articles.	Met	
CST-KM-009	Knowledge	Authoring	The supplier will ensure that articles can contain embedded links to other content within the Knowledge Base	Met	
CST-KM-010	Knowledge	Authoring	The supplier will ensure that versions of articles can be created in English and Welsh	Met	
CST-KM-011	Knowledge	Authoring	The supplier will ensure that broken links are highlighted to authors.	Met	
CST-KM-012	Knowledge	Authoring	The supplier will ensure that an audit history is retained and can be viewed for individual articles (e.g authoring team can record and review notes giving reasons for revision)	Met	
CST-KM-013	Knowledge	Authoring	The supplier will ensure that version history is kept on articles allowing authors to view and revert to old versions of an article.	Met	
CST-KM-014	Knowledge	Authoring	The supplier will ensure that designated users can archive and delete articles	Met	
CST-KM-015	Knowledge	Approval processes	The supplier will ensure that articles can be reviewed, checked, commented on and approved by subject matter experts before being published.	Met	
CST-KM-016	Knowledge	Notifications	The supplier will ensure that authors can notify groups of users when articles are changed or updated.	Met	
CST-KM-017	Knowledge	Notifications	The supplier will ensure that authors can require groups of users to read specific articles when these are published and confirming when read.	Met	

CST-KM-018	Knowledge	Notification MI	The supplier will ensure that MI can be produced on notifications, ensuring that mandatory content is read by users.	Met	
CST-KM-019	Knowledge	Access	The supplier will ensure that knowledge articles are available to staff that are not members of the Contact Centre	Met	
CST-KM-020	Knowledge	Access	The supplier will ensure that members of the public can only view public content	Met	
CST-KM-021	Knowledge	Access	The supplier will ensure public website access to content follows Government Digital Service (GDS) presentation guidelines	Met	
CST-KM-022	Knowledge	Access	The supplier will ensure that users can identify favourite articles with simple navigation to favourites.	Met	
CST-KM-023	Knowledge	Access	The supplier will ensure that users can manage favourite articles (e.g. change order).	Met	
CST-KM-024	Knowledge	Authoring	The supplier will ensure that designated users can create decision trees	Met	
CST-KM-025	Knowledge	Access	The supplier will ensure that article templates can be created and used to ensure consistency of format.	Met	
CST-KM-026	Knowledge	Search by keyword	The supplier will ensure that users can search for articles via keywords that match knowledge article content.	Met	
CST-KM-027	Knowledge	Searches	The supplier will ensure that users can submit natural language searches	Met	
CST-KM-028	Knowledge	Searches	The supplier will ensure that authors can create synomyns for search terms related to articles	Met	
CST-KM-029	Knowledge	Searches	The supplier will ensure that search facilities will support stemming (e.g. Apply, Applicant, Application)	Met	
CST-KM-030	Knowledge	Article ordering	The supplier will ensure that articles can be presented and ordered on best match to search and usage.	Met	
CST-KM-031	Knowledge	Navigate hierarchy	The supplier will ensure that users can search for content by navigating a hierarchy of article categories.	Met	

CST-KM-032	Knowledge	Feedback	The supplier will ensure that users can provide feedback on articles where the content may be in error or out of date.	Met	
CST-KM-033	Knowledge	Feedback	The supplier will ensure that when a user provides feedback then details of the user who left the feedback are captured too	Met	
CST-KM-034	Knowledge	Feedback	The supplier will ensure that authors can view lists of comments and questions raised, action and close these, removing the item once addressed.	Met	
CST-KM-035	Knowledge	Feedback	The supplier will ensure that if a user rates an article poorly then leaving comments is mandatory	Met	Articles that have been rated poorly will be presented for review.
CST-KM-036	Knowledge	Feedback	The supplier will ensure that users are able to provide feedback when searches don't provide useful or expected results	Met	Articles that have been rated poorly will be presented for review.
CST-KM-037	Knowledge	Feedback	The supplier will ensure that users can rate articles	Met	
CST-KM-038	Knowledge	Feedback	The supplier will ensure when feedback has been fixed/addressed notifications are sent to the user who provided the feedback	Met	
CST-KM-039	Knowledge	Feedback	The supplier will ensure that feedback submitted can be assigned for action to a specific designated user(s)	Met	
CST-KM-040	Knowledge	Expiry	The supplier will ensure that expiry time can be set for articles so that articles are automatically archived.	Met	
CST-KM-041	Knowledge	Expiry	The supplier will ensure that a review date can be set, when date reached a set of defined users are flagged to review and update article content.	Met	
CST-KM-042	Knowledge	Import/Export	The supplier will ensure that content can be imported from external documents in word or HTML.	Met	
CST-KM-043	Knowledge	Import/Export	The supplier will ensure that articles can be exported in open standard formats (e.g. Word, PDF, HTML, XML or similar).	Met	
CST-KM-044	Knowledge	MI	The supplier will ensure that the system reports on common search terms used to find articles and search terms that found no articles (to identify content gaps)	Met	
CST-KM-045	Knowledge	MI	The supplier will ensure that MI can be produced on the usage of articles.	Met	

CST-KM-046	Knowledge	MI	The supplier will ensure that MI can be produced on the activity of users, teams or groups	Met	
CST-KM-047	Knowledge	Publishing	The supplier will ensure that designated users can set a future date for content publication (e.g. pre-publish content).	Met	
CST-KM-048	Knowledge	Reporting	The supplier will ensure that reports can be run manually and scheduled to run	Met	
CST-KM-049	Knowledge	Reporting	The supplier will ensure that designated users can create and run custom reports	Met	
CST-KM-050	Knowledge	Reporting	The supplier will ensure that designated users can export reports	Met	
CST-KM-051	Knowledge	Content	The supplier will ensure that content can be reused across multiple articles	Met	
CST-KM-052	Knowledge	Internal AI	The supplier will ensure that the solution can extract meaning from article content and present answers to user questions, rather than simply displaying best fit articles.	Met	
CST-KM-053	Knowledge	External AI	The supplier will ensure that APIs allow integration of knowledge base content with external AI systems.	Met	
CST-KM-054	Knowledge	Contextual knowledge	The supplier will ensure that the knowledge solution can integrate with CCaaS and present agent assistance articles in response to customer interaction content when made available by the CCaaS solution. Content could include email text, webchat interactions or voice transcript data.	Met	

Non-Functional Requirements

01 - Integration					
Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partailly met	Comments
CST-INT-001	Access	Browser	The supplier will ensure the solution shall be accessible through HMCTS browsers; Google Chrome or Microsoft Edge	Met	
CST-INT-002	Access	Browser	The supplier will ensure the solution requires no desktop software installation (except for screen recording).	Met	
CST-INT-003	Access	Desktop	The supplier will ensure that any desktop software that needs to be installed on user equipment is capable of running on Windows 10 or higher.	Met	
CST-INT-004	Access	Accessibility	The supplier will ensure that the solution and all external and internal user interfaces (including but not limited to Customer, Agent, Workforce Management, Quality Management, Knowledge Authoring) provide accessibility as per current WCAG standards.	Met	
CST-INT-005	Access	Accessibility	The supplier will provide an up to date accessibility statement, stating compliance status outlined on: https://www.gov.uk/government/publications/sample-accessibility-statement	Met	
CST-INT-006	Access	Accessibility	The supplier will demonstrate a continuous commitment to review accessibility status in accordance with Government Accessibility standards outlined on: https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps	Met	
CST-INT-007	Access	Accessibility	The supplier will ensure that the solution is compatible with assistive technologies and must meet our minimum service standard requirements outlined on: https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies	Met	
CST-INT-008	Access	Accessibility	The supplier will ensure that all agent user interfaces provide accessibility as per assistive technologies standards requirements outlined on: https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies	Met	

CST-INT-009	Access	Accessibility	The supplier will ensure that administration and specialist role user interfaces (including but not limited to Workforce Management, Quality Management, Knowledge Authoring) provide accessibility as per assistive technologies standards requirements outlined on: https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies	Met	
CST-INT-010	Access	Accessibility	The supplier will ensure that all citizen facing interfaces and web sites are compatible with assistive technologies and must meet our minimum service standard requirements outlined on: https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies	Met	
CST-INT-011	Access	Accessibility	The supplier will ensure that all citizen facing interfaces can be configured so as to accommodate the UK Government Design System Standards	Met	
CST-INT-012	Integration	Data encryption	The supplier will ensure that all API's and integrations are secure using SSL certificates, TLS 2.1 or above and or secrets	Met	
CST-INT-013	Integration	Routing and queueing	The supplier will ensure that IVR, email and webchat routing and queuing flows can call out to external REST web services to perform business logic. The data within responses must be added to contact metadata for use by the contact flow logic.	Met	
CST-INT-014	Integration	Routing and queueing	The supplier will ensure APIs are provided that allow the Buyer's external applications to extract contacts from queues and assign and deliver the contact to a specific agent	Met	
CST-INT-015	Integration	Routing and queueing	The supplier will ensure that external API calls can be executed when a contact is delivered to an agent.	Met	
CST-INT-016	Integration	Routing and queueing	The supplier will ensure that their solution can integrate or ingest from HMCTS O365 Mailboxes using oAuth2, MSGraph or mail redirection	Met	
CST-INT-017	Integration	Configuration	The supplier will ensure that APIs are provided that allow the Buyer's external applications to lookup and retrieve details of the CCaaS configuration, particularly related to queues and agents.	Met	
CST-INT-018	Integration	Configuration	The supplier will ensure that REST web service APIs are provided that allow the Buyer's applications to edit and update queue and agent configuration.	Met	
CST-INT-019	Integration	WFM integration	The supplier will ensure that RTS APIs provide agent ACD status data that can be passed into an external WFM solution for adherence reporting.	Met	
CST-INT-020	Integration	WFM integration	The supplier will ensure that 15 minute queue data can be accessed to feed external WFM systems. Data fields to include but not limited to; date/time, channel, queue name, answered, abandoned, call volume, speed of answer, ring time, talk time, wrap time etc for all channel types.	Met	

CST-INT-021	Integration	MI data extract	The supplier will ensure that there is no limit on the data which can be transferred via the REST API's or provide mechanisms such as chunking or access to storage output via special one time links for larger data sets (e.g. Historical MI data).	Met	
CST-INT-022	Integration	MI data extract	The supplier will ensure that APIs and/or file export provides access to contact detail record and summarised data.	Met	
CST-INT-023	Integration	MI data extract	The supplier will ensure that schedule data (current and historical) and adherence MI can be extracted from WFM	Met	
CST-INT-024	Integration	SSO	The supplier will integrate CCaaS with the Buyer's Azure AD via SAML2.0 or other protocols supported by Azure AD for user authentication.	Met	
CST-INT-025	Integration	Security	The supplier will ensure that all inbound, outbound API traffic and authication is logged for security purposes	Met	
CST-INT-026	Integration	Security	The supplier will ensure that all API access can be limited to defined IP addresses / gateways supplied by the customer	Met	
CST-INT-027	Integration	Security	The supplier will ensure that they validate and sanitize user input to prevent SQL injection, XSS (Cross-Site Scripting), and other injection attacks	Met	
CST-INT-028	Integration	Security	The supplier will ensure that they Implement rate limiting to prevent abuse and protect against DDoS attacks from IP's not authorised by the client	Met	
CST-INT-029	Integration	Security	The supplier will ensure the secure storage and transmission of authentication tokens. Ensure they are properly hashed and salted when necessary	Met	
CST-INT-030	Integration	Security	The supplier will implement error handling to avoid leaking sensitive information in error messages. Return generic error messages to clients and log detailed errors on the server	Met	
CST-INT-031	Integration	Security	The supplier will ensure the use of versioning in the API design to ensure backward compatibility and to avoid breaking existing client applications when making changes	Met	
CST-INT-032	Integration	Performance	The supplier will ensure real time API response time will be < 1 second. For larger datasets call back mechanisms or polling may be implemented	Met	
CST-INT-033	Integration	Routing and queueing	The supplier will ensure that task requests can be submitted, updated and cancelled via APIs, with these tasks routed queued and presented to agents using the same capabilities as for voice, email and webchat.	Met	
CST-INT-034	Integration	Routing and queueing	The supplier will ensure that task submission APIs allow the buyer to define the parameters for the task. E.g. Task type, due date, priority, task URL, task notes, case id etc. This metadata must be available to use within routing logic.	Met	
CST-INT-035	Integration	External Services	The supplier will ensure the buyer is provided APIs to allow potential integration over the course of the contract between CCaaS and external Text to Speech services.	Met	

CST-INT-036	Integration	External Services	The supplier will ensure the buyer is provided APIs to allow potential integration over the course of the contract between CCaaS and external Transcription services.	Met	
CST-INT-037	Integration	External Services	The supplier will ensure the buyer is provided APIs to allow potential integration over the course of the contract between CCaaS and external Chatbot services.	Met	
CST-INT-038	Integration	External Services	The supplier will ensure the buyer is provided APIs to allow potential integration over the course of the contract between CCaaS and external Webchat services.	Met	
CST-INT-039	Integration	External Services	The supplier will ensure the buyer is provided APIs to allow potential integration over the course of the contract between CCaaS and external Knowledge solutions to provide contextual knowledge.	Met	
CST-INT-040	Telephony	Payments	The supplier will ensure that, if requested by the buyer, over the course of the contract, inbound or outbound calls can be transferred to a payment line when a payment needs to be taken.	Met	
CST-INT-041	Telephony	Payments	The supplier will, if requested by the buyer, over the course of the contract, provide telephony integration with a DTMF masking solution provider.	Met	
CST-INT-042	Telephony	Payments	The supplier will, if requested by the buyer, over the course of the contract, ensure that DTMF masking integration is limited to payment DDIs only.	Met	
CST-INT-043	Telephony	Payments	The supplier will, if requested by the buyer, over the course of the contract, ensure that the payment agent can enter DTMF to link the call to the payment (web) session.	Met	
CST-INT-044	Integration	Service Desk integration	The supplier will, if requested by the buyer, over the course of the contract, integrate their ITSM with the Buyer's ServcieNow cloud service for incident record synchronisation.	Met	

02 - Security

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partailly met	Comments
CST-SEC-001	Information Security Policies	Policy	The solution should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas).	Met	
CST-SEC-002	Information Security Policies	Policy	The supplier should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas).	Met	

CST-SEC-003	Organisation of Information Security	SPOC	The supplier must provide HMCTS with a Single Point Of Contact (SPOC) to act as coordinator and focal point for all the security aspects to the service and the SPOC (or a delegate) must be available to attend regular security working group meetings with HMCTS.	Met	
CST-SEC-004	Human Resource Security	Vetting and Clearance	The supplier must perform appropriate checks on all personnel involved in the design, delivery and operation of the solution (pre-employment, during employment, termination and change of employment) in order to ensure the security of HMCTS information assets and the safety of staff and individuals within HMCTS. At a minimum, personnel must successfully complete Baseline Personnel Security Standard (BPSS)(or equivalent) pre-employment screening before being granted access to HMCTS information assets (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard).	Met	
CST-SEC-005	Human Resource Security	Vetting and Clearance	The supplier must ensure all personnel (and those within the supply chain) hold the relevant vetting and clearance in accordance with the HMCTS Vetting and Clearance Policy (https://tools.hmcts.net/confluence/display/ISMS/Vetting+and+Clearance). The HMCTS SIRO must approve any departure from this. At a minimum, all personnel with access to (1) bulk personal data or administrative privileges will require Security Check (SC) clearance (2) Home Office or Policing systems will require Non-Police Personnel Vetting (NPPV) Clearance.	Met	
CST-SEC-006	Human Resource Security	Location	The supplier must ensure all personnel (and those within the supply chain) are based in the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.	Met	
CST-SEC-007	Human Resource Security	Training & Awareness	The supplier must ensure that all supplier and sub-contractor staff who have access to personal data, including staff in their supply chain if appropriate, undergo a session of data protection and information risk awareness training on induction and annually thereafter.	Met	
CST-SEC-008	Asset Management	Inventory	The supplier must produce and maintain an accurate inventory of information, system, hardware (where applicable) and software assets used to deliver the service.	Met	
CST-SEC-009	Asset Management	Data Classification	The supplier must implement measures to secure the physical handling, use, storage, transport and disposal of HMCTS information assets (whether in paper or electronic form) in accordance with the Government Security Classification Policy (https://www.gov.uk/government/publications/government-security-classifications) and SMP.	Met	

CST-SEC-010	Asset Management	Decommissioning	The supplier must decommission, dispose, sanitise or destruct infrastructure and data in accordance with National Cyber Security Centre (NCSC) guidance (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media). The supplier must provide a decommissioning approach document, at least 3 months ahead of the first planned decommissioning activity, detailing the decommissioning and disposal methodology for approval by HMCTS.	Met	
CST-SEC-011	Access Control	Authentication	The solution must implement secure authentication and authorisation mechanisms to reduce the likelihood of unauthorised access to the solution. At a minimum, the solution must support (1) Single Sign-on (SSO) (2) OAuth 2.0 (3) OpenID Connect (OIDC) (3) SAML2.0 (4) LDAPS (or equivalent).	Met	
CST-SEC-012	Access Control	Authentication	The solution must support or implement Multi-Factor Authentication (MFA). At a minimum, Time-based One-Time Password (TOTP) must be supported.	Met	
CST-SEC-013	Access Control	Authentication	Then solution must support user authentication to existing Identity and Access Management (IdAM) services used by HMCTS. At a minimum, the solution must (1) support Microsoft Entra ID (formerly Azure Active Directory) (2) respond to changes to user accounts or permissions within the HMCTS IdAM, within the minimum time possible (maximum 30 minutes).	Met	
CST-SEC-014	Access Control	Authorisation	The solution must provide the technical capability to configure a robust and granular Role Based Access Control (RBAC) model. At a minimum, the solution must provide the ability to (1) manage user permissions at an individual, team and group level (2) support Just-in-Time (JIT) access (3) enforce the Principle of Least Privilege (PoLP) (4) separate the request and approval stages of account creation (5) log changes to user permissions.	Met	
CST-SEC-015	Access Control	Privileged Access	The supplier must ensure segregation of duties by privileged users of the services. At a minimum this must include (1) ensuring the Principle of Least Privilege (PoLP) is always applied (2) ensuring separation of request and approval for account creation (3) logging changes to user permissions (4) regularly reviewing privileged user access (5) privileged accounts are unique to each user and must only be used when performing privileged actions.	Met	
CST-SEC-016	Access Control	JML	The solution must ensure that all user account management supports the HMCTS in securely onboarding new staff (Joiners), managing staff transitions between teams (Movers), and offboarding staff who leave the organisation (Leavers).	Met	

CST-SEC-017	Cryptography	Credentials and Secrets Management	The solution must provide a secure mechanism to store and retrieve credentials, cryptographic keys and secrets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/choosing-and-configuring-a-kms-for-secure-key-management-in-the-cloud). At a minimum, the solution must (1) use a tamper-resistant secure storage (2) provide a mechanism for automated rotation of keys and secrets (3) provide a mechanism for deletion or revocation of cryptographic keys (4) log and monitor access to cryptographic keys.	Met	
CST-SEC-018	Cryptography	Encryption (Data at rest)	The solution must implement cryptographic controls to provide data at rest protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience#principle23). At a minimum, the solution must (1) not use NIST deprecated or disallowed ciphers (2) support symmetric algorithm AES (3) support 256-bit key length (4) support AES-GCM or AES-XTS modes of operation (5) support SHA-256 hashing algorithm.	Met	
CST-SEC-019	Cryptography	Encryption (Data in transit)	The solution must implement cryptographic controls to provide data in transit protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data). At a minimum, the solution must (1) not use NIST deprecated ciphers (2) support TLS 1.2 or above (3) disable TLS features known to be insecure (4) support 2048-bit RSA or ECDSA-256 P-256 Curve signing algorithms (5) support SHA-256 hashing algorithm.	Met	
CST-SEC-020	Physical and Environmental Security	Physical and Environmental Security	The supplier must implement physical security controls at locations used in the provision of the solution and service. At a minimum, National Protective Security Authority (NPSA) guidance (https://www.npsa.gov.uk/advice-guidance) must be consulted to identify proportionate controls for preventing unauthorised physical access, damage and interference to information processing facilities where HMCTS data may be stored, processed and managed from.	Met	
CST-SEC-021	Operations Security	Malware	The solution must implement malware controls to detect and prevent malware-based attacks. At a minimum, the solution must (1) use up-to-date malware detection signatures or heuristics (2) prevent attacks in near real-time (3) be monitored to ensure malware controls are always enabled (4) meet NCSC pattern for Safely Importing Data (https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data) for any function designed to ingest, upload or store data from an untrusted source.	Met	

CST-SEC-022	Operations Security	Vendor Support	The supplier must ensure all software and hardware is supported by a vendor that produces regular security updates. At a minimum, the supplier must (1) inform HMCTS six months in advance of software or hardware reaching end of vendor support (2) inform HMCTS if extended support agreements have been purchased to obtain security updates.	Met	
CST-SEC-023	Operations Security	End User Devices	The supplier must ensure devices used to access or manage HMCTS data under the management authority of the supplier have a minimum set of security policy configurations enforced. At a minimum, all supplier devices must satisfy the security requirements set out in the NCSC Device Security guidance (https://www.ncsc.gov.uk/collection/device-security-guidance).	Met	
CST-SEC-024	Operations Security	Environments	The solution must enforce physical or logical segregation between production and non-production environments.	Met	
CST-SEC-025	Operations Security	SyOPs	The supplier must not extract/export any HMCTS data outside of the service, without written consent from HMCTS. Any HMCTS approved extract/export must be strictly controlled and recorded.	Met	
CST-SEC-026	Operations Security	Change Management	The supplier must ensure any changes to hardware and software configurations are performed under formal change control which includes security impact assessment prior to change approval. At a minimum, the supplier must audit against unauthorised changes at least once during any period of twelve months and provide evidence to HMCTS of audit findings.	Met	
CST-SEC-027	Operations Security	Audit, Logging and Monitoring	The solution must ensure security log events and audit events are retained and available for a configurable period. At a minimum, the solution must ensure security events and audit events (1) contain an accurate date and time stamp (2) are verbose enough to support effective security incident management and forensics (3) are stored and made available for a minimum of 90 days for services that can be accessed from the internet and a minimum of 13 months for services that are accessed using a MOJ, HMCTS or Government identity (5) should not be retained for longer than 2 years without specific approval from HMCTS.	Met	
CST-SEC-028	Operations Security	Security Monitoring	The supplier must ensure the solution is under 24x7x365 security monitoring to detect suspicious and unauthorised activities based on NCSC Security Monitoring guidance (https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)	Met	
CST-SEC-029	Operations Security	Security Monitoring	The supplier should provide an automated mechanism to export security event logs to HMCTS security monitoring systems.	Met	
CST-SEC-030	Operations Security	Technical Vulnerability Management	The supplier must perform regular vulnerability scanning of all the components within the solution. At a minimum, the scope must include (1) devices (2) infrastructure (3) software (4) firmware (5) software dependencies (6) application code analysis (SAST and DAST).	Met	

CST-SEC-031	Operations Security	Technical Vulnerability Management	The supplier must remediate all vulnerabilities in accordance with the HMCTS Vulnerability Management Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management). At a minimum CRITICAL severity vulnerabilities must be remediated as soon as reasonably practical (take first priority) and HIGH severity vulnerabilities remediated within 7 days.	Met	
CST-SEC-032	Operations Security	SyOPs	The supplier should comply with any Security Operating Procedures (SyOPs) that have been issued to HMCTS by organisations for which HMCTS processes data. At a minimum, this will include SyOPs from (1) Home Office (2) MoJ (3) Judiciary	Met	
CST-SEC-033	Operations Security	Technical Vulnerability Management	The supplier should provide regular reporting on vulnerability management. At a minimum, this should include information relating to (1) vulnerabilities detected (2) exploitability (3) mitigating controls (4) recommendations for remediation (4) remediation progress.	Met	
CST-SEC-034	Communications Security	Network Security	The solution must implement network security controls to make a network compromise difficult or reduce the impact of any network-based attack. At a minimum, controls must include (1) limiting all inbound and outbound traffic to only those sources/destinations and protocols required for the solution to function (2) network segmentation or zones (3) preventing lateral movement based on NCSC Preventing Lateral Movement Guidance (https://www.ncsc.gov.uk/guidance/preventing-lateral-movement) (4) preventing Denial-of-Service (DoS) attacks.	Met	
CST-SEC-035	System Acquisition, Development, and Maintenance	Risk Assessments	The supplier must produce and maintain an information security risk assessment of the solution based on a formal risk assessment methodology and share the output with HMCTS in the form of a documented information security risk register. At a minimum the risk assessment must include (1) risk events (2) risk causes (3) risk impact (4) risk severity (5) mitigating controls	Met	
CST-SEC-036	System Acquisition, Development, and Maintenance	System Interfaces	The solution must ensure any system-to-system data flows or Application Programming Interfaces (APIs) are protected using good practice security controls. At a minimum controls should include (1) authentication (2) integrity checking (3) encryption (4) limited data exposure (5) ensuring all third-party interfaces are covered by any MoU or other type of agreement.	Met	
CST-SEC-037	System Acquisition, Development, and Maintenance	Technical Design Documentation	The solution technical design documents issued to HMCTS must explicitly detail how HMCTS technical security non-functional requirements and outcomes are being implemented or met. At a minimum, all technical design documents must (1) include a dedicated security section (2) highlight any shortcomings against HMCTS technical security non-functional requirements (3) highlight any single point of failure that could impact the availability of the solution.	Met	

CST-SEC-038	System Acquisition, Development, and Maintenance	Secure Configuration	The solution components must be deployed and configured in accordance with any published and applicable secure deployment or configuration guides made available by Vendors, NCSC or Center for Internet Security (CIS). For example: Microsoft Cloud Security Benchmark (https://learn.microsoft.com/en-us/security/benchmark/azure/) AWS Security Documentation (https://docs.aws.amazon.com/security/) NCSC Device Security Guidance for Windows (https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows) CIS Benchmark for RHEL (https://www.cisecurity.org/benchmark/red_hat_linux)	Met	
CST-SEC-039	System Acquisition, Development, and Maintenance	NCSC CSP	The solution must meet all applicable requirements of the NCSC Cloud Security Principles (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles). At a minimum, all mutli-tenant cloud services must demonstrate how tenant separation or boundaries are implemented within compute, storage and data flows and networking.	Met	
CST-SEC-040	System Acquisition, Development, and Maintenance	NCSC CAF	The supplier should share security related information about the solution in order to assist HMCTS in completing the NCSC Cyber Assessment Framework (CAF)(https://www.ncsc.gov.uk/collection/caf)	Met	
CST-SEC-041	System Acquisition, Development, and Maintenance	NCSC SDP	The solution must demonstrate implementation of the NCSC Secure Design Principles (https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles).	Met	
CST-SEC-042	System Acquisition, Development, and Maintenance	NCSC BPD	The solution must demonstrate applicable measures have been implemented from the NCSC Protecting Bulk Personal Data Guidance (https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data).	Met	
CST-SEC-043	System Acquisition, Development, and Maintenance	OWASP	The solution must ensure any web applications and APIs are designed and implemented to prevent common security attacks such as those listed in the OWASP Top 10 (https://owasp.org/www-project-top-ten/).	Met	
CST-SEC-044	System Acquisition, Development, and Maintenance	Test Data	The solution must ensure live HMCTS data (or copies of) are only stored in production (operational) systems.	Met	

CST-SEC-045	Supplier Relationships	Contracts	The supplier must ensure, and provide evidence to HMCTS, that all security requirements – functional and non-functional – applicable to the solution or service, will flow down in the supply chain and will apply to all sub-contractors, partners, and suppliers that participate in the solution or service.	Met	
CST-SEC-046	Information Security Incident Management	Process	The supplier and HMCTS must notify the other upon becoming aware of any security incident, breach of security or any potential or attempted breach of security (including throughout the supply chain) in accordance with the ISMS, SMP and HMCTS Security Incident Management Policy (https://tools.hmcts.net/confluence/display/ISMS/Security+Incident+Management).	Met	
CST-SEC-047	Information Security Aspects of Business Continuity Management	BCMS	The supplier must develop and maintain a Business Continuity and Disaster Recovery Plan that meets the requirements of ISO/IEC22301 (https://www.iso.org/standard/75106.html). The Plan must be specific to the service delivered to HMCTS.	Met	
CST-SEC-048	Information Security Aspects of Business Continuity Management	Testing backups	The supplier must test backup solutions. At a minimum this must include (1) a backup test at least every three months (2) verifying data reliability and integrity of data in scope of the ISMS (3) ensuring that any testing meets the requirements of the BCDR plan (4) verifying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) can be met.	Met	
CST-SEC-049	Compliance	SMP	The supplier must prepare, develop, maintain and deliver HMCTS for approval a complete and up to date Security Management Plan (SMP) covering all services delivered under contract. At a minimum, the SMP must (1) be structured in accordance with the HMCTS SMP template (https://tools.hmcts.net/confluence/display/ISMS/SMP+Template) (2) identify how the supplier's ISMS applies to the services offered to HMCTS (3) explicitly detail how security non-functional requirements and outcomes are being implemented or met (4) identify the necessary delegated organisational roles defined for those responsible for delivering and overseeing the SMP (5) detail the supplier approach and processes for delivering the services using Sub-Contractors and third parties authorised by HMCTS.	Met	
CST-SEC-050	Compliance	SAL	The supplier must ensure that all changes to services impacting IT security are approved in accordance with the agreed change procedure and take account of the latest Security Aspects Letter (SAL)(https://tools.hmcts.net/confluence/display/ISMS/SAL+Template).	Met	

CST-SEC-051	Compliance	ISMS	The supplier must hold and maintain valid ISO 27001 certification for their Information Security Management System (ISMS). The certification must be issued by a UKAS registered certification body the scope of which fully and explicitly includes the system(s) used for the solution, service and data and all related operations and procedures.	Met	
CST-SEC-052	Compliance	Cyber Essentials	The supplier must hold and maintain Cyber Essentials (CE) Plus certification the scope of which includes the systems within the solution provided to HMCTS.	Met	
CST-SEC-053	Compliance	Technical Vulnerability Management	The supplier must perform an IT Health Check (ITHC) of the solution under the CHECK scheme (https://www.ncsc.gov.uk/information/check-penetration-testing). At a minimum, this must include (1) performing an ITHC within the last six months of service commencement, thereafter annually and upon significant change to the system (or a system component) (2) a scope that contains all components within the solution or a subset that has been approved by HMCTS (3) sharing ITHC report findings with HMCTS (4) remediation of all discovered vulnerabilities in accordance with the HMCTS Vulnerability Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management)	Partially met	Access to Genesys Cloud is permitted for customers to perform an IT Health Check. Kerv will work with HMCTS to perform this check under the CHECK scheme. Genesys provide customer with access to their penetration test results. These tests are carried out by Genesys under international standards.
CST-SEC-054	Compliance	Data Protection	The solution must ensure all HMCTS data is stored, supported and processed within the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.	Met	
CST-SEC-055	Compliance	Data Protection	The supplier must ensure that all aspects of the service provided to HMCTS is performed in accordance with Data Protection Legislation (UK GDPR and UK DPA), comply with both the law and good practice, respect the rights of individuals, be open and honest about how it handles personal data.	Met	
CST-SEC-056	Compliance	HMCTS Audit and Inspection	The supplier must allow for audits and inspections of its data processing activity by HMCTS or an auditor designated by HMCTS.	Met	
CST-SEC-057	Compliance	PCI DSS	The supplier must comply with the requirements of the Payment Card Industry Data Security Standards (PCI DSS) where applicable to the solution.	Met	
CST-SEC-058	Compliance	Internal audit	The supplier should conduct internal security audits from time to time (and at least annually) across the scope of the ISMS and additionally after any change or amendment to the ISMS or SMP. At a minimum, security audit findings should be shared with HMCTS in the form of a report.	Met	
CST-SEC-059	Compliance	Detailed Security Requirements	The supplier must comply with HMCTS Detailed Security Requirements provided with the contract.	Met	

03 - Implementation

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partailly met	Comments
CST-IMP-001	Implementation	Mobilisation	The Supplier shall, by the end of the Mobilisation, appoint an appropriately qualified test manager who shall be fully accountable for all testing performed and/or supported by the Supplier during the project. Where possible, the Supplier shall ensure continuity of the identified test manager throughout the project.	Met	
CST-IMP-002	Implementation	Mobilisation	The Supplier shall, by the end of Mobilisation, appoint a Delivery/Project lead who shall: a) manage the Supplier responsibilities within the project; b) supervise the conduct of the project on behalf of the Supplier; c) take full accountability for project delivery on behalf of the Supplier; d) liaise with the Buyer on behalf of the Supplier; e) provide assistance to the Buyer's project delivery manager in the communication with and coordination of the Buyer's resources required to achieve the implementation; f) ensure provision of a communication plan and assist the Buyer's project delivery manager in communicating with end users and the Buyer's stakeholders throughout the project; and g) maintain all project records including logs for incidents, risks and issues.	Met	
CST-IMP-003	Implementation	Mobilisation	The Supplier shall, by the end of the Mobilisation, appoint a named, and suitably qualified, point of contact, as a Business Change resource, through whom delivery of business change services (e.g. training, comms) will be managed on a day-to-day basis. Where possible, the Supplier shall ensure continuity of the identified test manager throughout the project.	Met	

CST-IMP-004	Implementation	Mobilisation	The Supplier shall, by the end of the Mobilisation, set up a programme management office that shall: a) operate for the duration of the Transition; b) adhere to standards and processes as outlined by the Buyer and agreed as part of the Implementation Plan; c) have a scope of activity that includes: I. resource recruitment; II. set up of project infrastructure and customisation of tools and templates; III. reporting processes and procedures; IV. planning processes and standards; V. resource management processes and procedures; VI. quality management processes and procedures; VII. risk management processes and procedures; VIII. change management processes and procedures; IX. library and document management processes and procedures; X. Transition communication plan; and XI. Planning of communication with the Buyer	Met	
CST-IMP-005	Implementation	Mobilisation	The Supplier shall, by the end of Mobilisation, complete technical and business discovery, analysis and due diligence on topics including but not limited to; routing and queueing methodology, contact presentation, ways of working, knowledge taxonomy, wfm processes, quality processes etc.	Met	
CST-IMP-006	Implementation	Mobilisation	The supplier shall by the end of Mobilisation provide the Buyer with an Implementation Plan to include scope, releases and deliverables, delivery approach, test strategy, approach to training and communications, resources, supplier management project timeline, dependencies and milestones.	Met	
CST-IMP-007	Implementation	Mobilisation	The Supplier shall, in accordance with the Implementation Plan: a) provide a report on the discovery, analysis and due diligence exercise b) include findings in the report relevant to delivering the solution; c) inform the Buyer of any potential impact on the solution; and d) engage with the Buyer to determine an agreeable solution to resolve issues as part of the Implementation Plan.	Met	

CST-IMP-008	Implementation	Mobilisation	The Supplier shall ensure that the project initiation document provided to the Buyer, in accordance with the Implementation Plan, includes: a) the outlining of project objectives and outcomes; b) scope; c) approach; d) key activities; e) key assumptions; f) team organisational structure; g) key stakeholders and communication strategy; h) change management approach; and i) Project controls.	Met	
CST-IMP-009	Implementation	Mobilisation	The Supplier shall, by the end of Mobilisation, provide the Buyer with a detailed RACI (responsible, accountable, consulted, informed) matrix based in part on Buyer input.	Met	
CST-IMP-010	Implementation	Design, Development & Test	The Supplier shall, in accordance with the Implementation Plan, provide the Buyer with a Service Management plan that demonstrates how it shall meet its contractual obligations in relation to in-life delivery and support of the Services including Service Levels and Performance Monitoring requirements as set out elsewhere in this set of requirements (Service Levels).	Met	
CST-IMP-011	Implementation	Design, Development & Test	The buyer needs to be able to access facilities for development (of buyer's solutions), perform unit testing, perform user acceptance testing, manage and test configuration changes, promotion to a production solution and provide user training. The Supplier shall, in accordance with the Implementation Plan, detail their approach to the provision of these facilities with an approach that ensures there is no impact to live configuration, data or performance.	Met	
CST-IMP-012	Implementation	Design, Development & Test	The Supplier shall ensure that the facilities are representative of the production environment i.e. same versions and consistent capabilities. The buyer requires the ability to train at least 30 concurrent users and require the ability to test with up to 20 concurrent users.	Met	
CST-IMP-013	Implementation	Design, Development & Test	The Supplier shall provide the Buyer with high and low level technical designs in accordance with the Implementation Plan.	Met	
CST-IMP-014	Implementation	Design, Development & Test	The Supplier shall obtain agreement from the Buyer's technical design authority for all technical and service designs, and any subsequent updates to them, prior to their implementation.	Met	
CST-IMP-015	Implementation	Design, Development & Test	In accordance with the Test Strategy (Implementation Plan) the Supplier shall provide Test plans and Test specifications for solution testing.	Met	

CST-IMP-016	Implementation	Design, Development & Test	The supplier shall produce test phase artefacts for review and approval including Test Plans, Test Scripts and Test Reports.	Met	
CST-IMP-017	Implementation	Design, Development & Test	The Supplier shall ensure that interfaces with external service components are tested as soon as they are connected rather than waiting for system integration testing i.e. de-risk system integration testing.	Met	
CST-IMP-018	Implementation	Design, Development & Test	The Supplier shall undertake appropriate unit/component, platform, information security, integration, operational acceptance and service acceptance Testing. The outcomes of testing must be shared with the Buyer.	Met	
CST-IMP-019	Implementation	Design, Development & Test	The Supplier shall design, deliver and operate its solution and Implementation Plan such that it supports test assurance activities conducted by the Buyer without adversely impacting the project and/or Service acceptance and/or performance against the Service Levels and/or performance against the KPIs.	Met	
CST-IMP-020	Implementation	Design, Development & Test	The Supplier shall undertake appropriate Service Management, user acceptance and end to end (unstructured) Testing of the solution with the Buyer's delivery team to ensure that their solution is ready for all required Operational Service Commencement Dates and supporting rectification of Test Issues before the relevant Operational Service Commencement Date. The Supplier shall be responsible for supporting the Buyer in the planning, design, implementation, execution and reporting of the Service Management, User Acceptance and end-to-end Testing.	Met	
CST-IMP-021	Implementation	Design, Development & Test	The Supplier shall build and configure the solution in line with the specified requirements and agreed designs including the technical designs.	Met	
CST-IMP-022	Implementation	Design, Development & Test	The Supplier shall engage with HMCTS's encumbent suppliers to successfully design and implement the solution.	Met	
CST-IMP-023	Implementation	Design, Development & Test	The Supplier shall provide consultancy services to the Buyer during the configuration and setup of the solution.	Met	

CST-IMP-024	Implementation	Design, Development & Test	The Supplier shall contribute to and support the development of an appropriate Roles Based Access Control matrix for the solution.	Met	
CST-IMP-025	Implementation	Training	The Supplier shall, in accordance with the Implementation Plan, provide the Buyer with a training approach and plan which shall include: a) analysis of training needs and subsequent identification of appropriate training; and b) the Supplier approach to meeting the training needs including: i. how training materials will be developed; and ii. how training will be deployed to Buyer stakeholder groups and end users whilst ensuring that training does not impact continuity of service.	Met	
CST-IMP-026	Implementation	Training	The Supplier shall produce and agree with the Buyer suitable training material and knowledge articles.	Met	
CST-IMP-027	Implementation	Training	The Supplier shall provide instructor led training/directed learning options to the Buyer.	Met	
CST-IMP-028	Implementation	Training	The Supplier shall provide onsite training options to the Buyer.	Met	
CST-IMP-029	Implementation	Training	The Supplier shall provide remote training options to the Buyer.	Met	
CST-IMP-030	Implementation	Training	The Supplier shall provide online training materials to the Buyer.	Met	
CST-IMP-031	Implementation	Training	The Supplier shall provide training to the relevant end users and other parties, as agreed with the Buyer.	Met	
CST-IMP-032	Implementation	Training	The Supplier shall provide best practice guidance/specialist training to relevant end users and other parties, as agreed with the Buyer.	Met	
CST-IMP-033	Implementation	Transition	The Supplier shall, in accordance with the Implementation Plan, support the Buyer with people related change management, including provision of change and communication plans.	Met	
CST-IMP-034	Implementation	Transition	The Supplier shall plan, manage, and seamlessly deliver the orderly transition from the preceding solution in an approach to be agreed with the Buyer in the Implementation Plan.	Met	

CST-IMP-035	Implementation	Transition	The Supplier shall co-ordinate and manage the transition off the preceding solution, including requesting from the Buyer the co-ordination of inputs required from other Suppliers to deliver the transition off the preceding solution.	Met	
CST-IMP-036	Implementation	Transition	The Supplier shall plan and conduct transition such that it does not adversely impact the services that have already become operational Services, including their performance in accordance with required Service Levels.	Met	
CST-IMP-037	Implementation	Transition	The Supplier shall plan and conduct implementation and transition such that it does not adversely impact the preceding solution including its service management arrangements and processes, procedures and tooling which should be in place and fully functional throughout the transition until the relevant Operational Service Commencement Dates for the solution.	Met	
CST-IMP-038	Implementation	Transition	The Supplier shall plan and conduct implementation and transition such that it does not adversely impact Services and their business operations and it allows those Services to maintain their service continuity through consideration of factors including: the Services' ability to maintain minimum resource levels required during training; and avoiding impact on the Operational Service.	Met	
CST-IMP-039	Implementation	Transition	The Supplier shall contribute to and support the Acceptance into Service reviews process including Service readiness review(s), confirming the completion of the implementation activities and that the Supplier has all the requisite credentials, knowledge, and systems expertise to commence the scope of Management Services, including: 1) Implementation status for post Operational Service Commencement Date operations; 2) Day to day operational and Service Management readiness; 3) Operational status of Service Management processes, tools, monitoring methods, events and alerts, sufficient to deliver Service Management capability for Operational Service Commencement; and 4) Service continuity plans and evidence of testing. Items 1 to 4 are to be Approved by the Buyer	Met	
CST-IMP-040	Implementation	Transition	The Supplier shall provide to and seek approval from the Buyer for a Cutover Plan(s) that covers the pre- and post- period of Operational Service Commencement Date for each of the Services and includes: a) the activities required to transition each Service; b) the timings and resources required to cutover to the solution; and c) a level of detail which provides the Buyer with assurance on the Supplier ability to meet Operational Service Commencement Dates.	Met	

CST-IMP-041	Implementation	Transition	The Supplier shall provide to, and seek approval from the Buyer for, an Early Life Support plan for any new Operational Service or change to existing Operational Services. The Early Life Support plan shall detail: a) activities, resources, communications and escalation paths that will occur post Operational Service Commencement Date prior to exit of Early Life Support; and b)criteria for stabilisation of the Services.	Met	
CST-IMP-042	Implementation	Transition	The Supplier shall provide the Buyer, in a format agreed with the Buyer, a final post-Operational Service Commencement Date report that includes a summary of the Operational Services activities carried out by the Supplier since the Operational Service Commencement Date and the status of the solution, within five (5) Working Days of the Operational Service Commencement Date for each Service.	Met	
CST-IMP-043	Implementation	Transition	The Supplier shall participate and contribute to post Operational Service Commencement Date reviews for each Service.	Met	
CST-IMP-044	Implementation	Transition	The Supplier shall, if requested, provide the Buyer resource for onsite floorwalking activities for a period of two (2) days for each site delivering the Service.	Met	
CST-IMP-045	Implementation	Transition	The Supplier shall provide Performance Monitoring during Early Life Support.	Met	
CST-IMP-046	Implementation	Transition	The Supplier shall ensure that appropriate resources are mobilised and available during Early Life Support in order to resolve operational and support issues quickly and reduce the amount of unavailability while enhancing acceptability of the solution by the end users.	Met	
CST-IMP-047	Implementation	Transition	The Supplier shall provide Early Life Support for a period of one (1) week from the Operational Service Commencement Date for each Service.	Met	
CST-IMP-048	Implementation	Transition	The Supplier shall, to exit Early Life Support, complete activities including: completing the acceptance process, seeking service readiness from the Buyer, and executing service transfer plans.	Met	
CST-IMP-049	Implementation	Project Delivery	The Supplier shall plan and conduct implementation and transition such that it does not adversely impact the preceding solution and their continued delivery to their standards and levels of service.	Met	

CST-IMP-050	Implementation	Project Delivery	Where required by the Buyer, the Supplier shall participate in the Buyer's governance forums.	Met	
CST-IMP-051	Implementation	Project Delivery	The Supplier shall engage and comply with a joint project delivery governance forum including: i. jointly undertake the governance of the project; ii. confirm Milestone completions and to act as an escalation point; iii. select an escalation group in case the joint project delivery governance cannot resolve all issues; iv. deal with all aspects of project delivery including other suppliers, site-cooperation, information exchanges etc; vi. discuss changes requested by the Supplier or the Buyer; vii. meeting regularly at a specified cadence; and viii.issue meeting minutes.	Met	
CST-IMP-052	Implementation	Project Delivery	The Supplier shall, as agreed in the Implementation Plan, provide a report that: a) is in the agreed format; b) is provided on a weekly basis for review during a weekly meeting, unless another cadence is agreed; and c) provides updates to the Buyer on the progress of the project including but not limited to: i. resourcing and mobilisation; ii. progress against Implementation Plan; and iii.RAID (risks, assumptions, issues and dependencies).	Met	
CST-IMP-053	Implementation	Project Delivery	The Supplier shall develop a detailed Project Delivery Plan. The Supplier's Implementation Plan shall, unless otherwise agreed with the Buyer, include key Milestone dates and should incorporate activities, deliverables and milestones associated with aspects including technical, service, commercial, finance, people and testing.	Met	
CST-IMP-054	Implementation	Project Delivery	The Supplier shall develop a Project Delivery Plan that provides an optimal approach to a speedy delivery of all releases of the solution. Where possible, the Supplier shall ensure continuity of the resources throughout the project.	Met	
CST-IMP-055	Implementation	Project Delivery	The Supplier shall obtain security authority to operate (ATO) by the date of the relevant Milestone in the Delivery Plan which may include obtaining certification and/or accreditation from an external accreditor.	Met	

CST-IMP-056	Implementation	Project Delivery	The Supplier's detailed Project Delivery Plan shall have the following attributes, to be Approved by the Buyer: a) be in MS Project readable format or other formats prescribed by the buyer; b) be fully resourced, identifying resource names where possible; c) show the critical path including the Transition Milestones d) locate and demonstrate implicit and explicit contingencies; e) identify and agree any dependencies on the Buyer and/or the Buyer's stakeholders and/or Other Suppliers including providers of Preceding Solution; f) be constructed in such a way that a weekly consolidated work plan showing exact progress against each task can be reported to the Buyer; and g) be constructed in such a way that any impact on the Supplier's ability to achieve the Milestones is reported to the Buyer on a weekly basis.	Met	
CST-IMP-057	Implementation	Project Delivery	The Supplier shall, in accordance with the Implementation Plan, provide the Buyer with a communication plan which addresses the approach to each stakeholder and stakeholder group. The Supplier shall engage with the Buyer to identify all relevant stakeholders and stakeholder groups to whom communications shall be required during the project in order to support a smooth and orderly transition.	Met	
CST-IMP-058	Implementation	Project Delivery	The Supplier shall, in accordance with the Implementation Plan, provide, to be Approved by the Buyer, a supplier management approach and plan describing activities and steps necessary with regard to sub-contractors to facilitate the Supplier's Implementation Plan.	Met	
CST-IMP-059	Implementation	Project Delivery	The Supplier shall actively participate in lessons learnt review to inform future delivery and implementation activities and continuously improve the Services for the Buyer.	Met	
CST-IMP-060	Implementation	Project Delivery	The Supplier shall provide the Buyer with a project closure report which details the completion of activities identified in the Implementation Plan and their Approval by the Buyer within the dates specified in the Implementation Plan.	Met	
CST-IMP-061	Implementation	Project Delivery	Where requested by the Buyer and following the Operational Services Commencement Dates, the Supplier shall support the Buyer with the closure of the project.	Met	

04 - Service Management

Ref No	Level 0 Category	Level 1 Category	Requirement	Met/not met/partailly met	Comments
CST-SRVMGNT-001	Service Management	General Service Management	The Supplier shall operate a governance structure that reflects the Buyer's governance structure requirements with appropriate management escalation points.	Met	
CST-SRVMGNT-002	Service Management	General Service Management	The Supplier shall provide support, as defined and agreed between both parties, in order to maintain their Service Management Policies, Processes and Procedures throughout the "call off contract" period.	Met	
CST-SRVMGNT-003	Service Management	Availability Management	The Supplier shall provide an application availability for normal business use, in line with the HMCTS specified availability targets of 99.99% during service hours (Carrier Services, CCaaS, KMS and Payment Handling).	Met	
CST-SRVMGNT-004	Service Management	Availability Management	The Supplier shall provide an application availability for normal business use, in line with the HMCTS specified availability targets of 99.90% during service hours (WFM)	Met	
CST-SRVMGNT-005	Service Management	Availability Management	The Supplier shall provide an application availability, in line with the HMCTS specified service hours (e.g. 'Mon-Fri 7am to 9pm' and 'Sat 7am to 5pm')	Met	
CST-SRVMGNT-006	Service Management	Availability Management	The Supplier shall provide proactive monitoring and reporting to achieve the agreed service availability.	Met	
CST-SRVMGNT-007	Service Management	Capacity Management	The supplier will ensure that the solution can provide capacity of at least that stated in the volumetrics +50%	Met	
CST-SRVMGNT-008	Service Management	Capacity Management	The Supplier shall proactively manage the infrastructure capacity of the solution based on the service performance, ensuring demand can be met.	Met	
CST-SRVMGNT-009	Service Management	Capacity Management	The Supplier must be able to deliver a performant service to accommodate expected user volumes as defined in the volumetrics document.	Met	
CST-SRVMGNT-010	Service Management	Capacity Management	The Supplier must be able to deliver a performant service in line with the following response times for user interface interactions: System response time target for user interface interactions: 1 sec (90th percentile) 1.5 sec (95th percentile) 2 sec (99th percentile)	Met	

CST-SRVMGNT-011	Service Management	Change Management	The Supplier must be equal to or better than the HMCTS change management success rate targets in relation to submission being no less then 48 hours on planned works and 5 working days for PIR (Post Implementation Review) submissions.	Met	
CST-SRVMGNT-012	Service Management	Change Management	The Supplier shall engage with the eRFC (emergency request for change) process in accordance with HMCTS process and provide full clarity of detail ahead of any changes required. This will relate to changes which are time critical and may include a change to resolve a major incident or apply an urgent security patch.	Met	
CST-SRVMGNT-013	Service Management	Release Management	The Supplier will inform HMCTS of any releases 14 days prior and provide visibility of their roadmap for a period of 3 months.	Met	Note - Genesys provides 7 days notice of new feature deployments.
CST-SRVMGNT-014	Service Management	Release Management	The Supplier shall work and collaborate with the Buyer to plan and implement release activity to ensure that any business disruption is minimised.	Met	
CST-SRVMGNT-015	Service Management	Incident Management	The Supplier shall provide progress updates for all P3 and P4 incidents in line with DTS default service level agreement. 98% of Priority Level 3 Incident Records are updated every (2) Business Days until the Incident has been resolved or the Priority Level has been changed 98% of Priority Level 4 Incident Records are updated every (2) Business Days until the Incident has been resolved or the Priority Level has been changed	Met	Note - Please refer to Schedule 9 in this call off contract which defines the SLA's to be delivered and replaces this requirement
CST-SRVMGNT-016	Service Management	Incident Management	The Supplier's incident management should integrate with the HMCTS incident management process for P3 and P4 incidents and issue initial and update communications according to service level agreement. 90% of P3's are resolved within 16 hours 98% of P3's are resolved within 24 hours 90% of P4's are resolved within 35 hours 98% of P4's are resolved within 70 hours	Met	Note - Please refer to Schedule 9 in this call off contract which defines the SLA's to be delivered and replaces this requirement
CST-SRVMGNT-017	Service Management	Incident Management	The Supplier shall align to the HMCTS incident management process to ensure joint management and resolution of P3 and P4 incidents.	Met	

CST-SRVMGNT-018	Service Management	Major Incident Management	The Supplier shall provide progress updates on P1 and P2 major incidents to the HMCTS major incident management function according to DTS default service level agreement. 98% of promoted P1 major incidents have initial communication sent within 30 minutes 98% of promoted P1 major incidents have update communications sent within 60 minutes of previous communications 98% of promoted P2 major incidents have initial communication sent within 60 minutes 98% of promoted P2 major incidents have update communications sent within 120 minutes of previous communications	Met	
CST-SRVMGNT-019	Service Management	Major Incident Management	The Supplier shall align with the HMCTS major incident management process to ensure joint management and resolution of P1 and P2 major incidents. 90% of P1's are resolved within 4 hours 98% of P1's are resolved within 8 hours 90% of P2's are resolved within 8 hours 98% of P2's are resolved within 12 hours	Met	Note - Please refer to Schedule 9 in this call off contract which defines the SLA's to be delivered and replaces this requirement
CST-SRVMGNT-020	Service Management	Major Incident Management	The Supplier shall align to the HMCTS incident management process to ensure joint management and resolution of P1 and P2 incidents.	Met	
CST-SRVMGNT-021	Service Management	Knowledge Management	The Supplier shall collaborate on / provide knowledge articles to the HMCTS service desk (through various methods including integration and importation) and ensure all relevant service desk personnel and service users are able to obtain the right knowledge, at the right time to support the solution used by HMCTS.	Met	
CST-SRVMGNT-022	Service Management	Knowledge Management	The Supplier shall provide any subsequent new knowledge articles, and updates to any existing knowledge articles, to the HMCTS service desk.	Met	
CST-SRVMGNT-023	Service Management	Problem Management	The Supplier will have a problem management process which will include the provision of root cause analysis information and can be reported on as part of monthly service reviews.	Met	
CST-SRVMGNT-024	Service Management	Problem Management	The Supplier should have a dedicated problem management resource working with HMCTS problem management.	Met	
CST-SRVMGNT-025	Service Management	Problem Management	The Supplier should provide root cause analysis information within 10 working days for all P1/P2 incidents.	Met	

CST-SRVMGNT-026	Service Management	Request Fulfilment	The Supplier shall provide a request fulfilment capability with management and coordination of all service requests that are agreed under the service remit, complying to the HMCTS request fulfilment process and agreed service levels.	Met	
CST-SRVMGNT-027	Service Management	Request Fulfilment	The Supplier shall fulfil service requests via the service catalogue in line with the service level agreement.	Met	
CST-SRVMGNT-028	Service Management	Request Fulfilment	The Supplier shall have a collaborative input into identifying, documenting and creating these catalogue items, alongside the HMCTS teams who own the request catalogue process.	Met	
CST-SRVMGNT-029	Service Management	Service Desk	The Supplier service desk must be equal to or better than the HMCTS first-contact resolution service level agreement of 70%.	Not met	As HMCTS would be the first point of contact for users, any simple issues would be resolved there. Therefore, issues escalated to Kerv would require investigation to resolve and the First Contact Resolution (FCR) rate would be below 70%. Kerv has provided the Genesys Beyond training subscription which will enrich the knowledge and capabiltiy of the HMCTS service desk improving the FCR.
CST-SRVMGNT-030	Service Management	Service Desk	The Supplier's service desk shall be rated / certified by Service Desk Institute (SDI)	Not met	Kerv Experience has previously reviewed the SDI certificate and the certification is on our roadmap.
CST-SRVMGNT-031	Service Management	Service Desk	The Supplier should hold ISO/IEC 20000 certification and proactively maintain the skills and knowledge.	Not met	Kerv Experience is currently working towards ISO/IEC 20000 certification.
CST-SRVMGNT-032	Service Management	Integration	The Supplier shall ensure any integrations conform to the HMCTS core or required ITIL processes to provide effective service management.	Met	
CST-SRVMGNT-033	Service Management	Certificate Management	The Supplier shall perform certificate management which aligns with the HMCTS certificate management requirements. Where certificates are required from HMCTS the supplier must engage with HMCTS certificate management process. The supplier must ensure that call certificate end dates are monitored and new certificates requested to ensure that no certificate has < 30 days left to run.	Met	
CST-SRVMGNT-034	Service Management	Application Monitoring	The Solution must have full stack monitoring in place.	Met	

CST-SRVMGNT-035	Service Management	Application Monitoring	The solution should have real user journey monitoring.	Met	
CST-SRVMGNT-036	Service Management	Application Monitoring	The Supplier will allow HMCTS to perform external monitoring using published interfaces.	Met	
CST-SRVMGNT-037	Service Management	Service Level Management	The Supplier shall measure suitable key performance indicators (KPIs) aligned to the HMCTS incident process performance KPIs, for the agreed reporting period and in line with the HMCTS information and data standards and the service levels agreed with the Supplier.	Met	
CST-SRVMGNT-038	Service Management	Service Level Management	The Supplier shall measure suitable KPIs aligned to the HMCTS problem process performance KPIs, for the agreed reporting period and in line with the HMCTS information and data standards and the service levels agreed with the Supplier.	Met	
CST-SRVMGNT-039	Service Management	Service Level Management	The Supplier shall measure suitable KPIs aligned to the HMCTS change process performance KPIs, for the agreed reporting period and in line with the HMCTS information and data standards and the service levels agreed with the Supplier.	Met	
CST-SRVMGNT-040	Service Management	Service Measurement and Performance Management	The Supplier will ensure data and reporting for the solution for the agreed reporting period includes performance against availability % of actual and expected targets, and in line with the HMCTS information and data standards.	Met	
CST-SRVMGNT-041	Service Management	Service Measurement and Performance Management	The Supplier's service desk shall provide service level reporting of performance against agreed metrics as per 'process integration' requirements, for the agreed reporting period and in line with the HMCTS information and data standards.	Met	
CST-SRVMGNT-042	Service Management	Service Measurement and Performance Management	The Supplier shall include performance related data in management information reporting for the agreed reporting period and in line with the HMCTS information and data standards.	Met	
CST-SRVMGNT-043	Service Management	Service Measurement and Performance Management	The Supplier shall provide regular reporting to HMCTS on the performance of the solution to agreed KPIs for known problems, incident resolution, active changes, and service requests relating to the solution and in line with the HMCTS information and data standards.	Met	
CST-SRVMGNT-044	Service Management	Supplier Management	The Supplier will facilitate a recurring monthly Service review meetings and will present the Service performance report. The service report should be ready and sent for review 5 working days before the monthly service review meeting.	Met	Note - Please refer to Schedule 9 in this call off contract which defines the SLA's to be delivered and replaces this requirement
CST-SRVMGNT-045	Service Management	Testing	The Supplier shall work with HMCTS to facilitate testing after upgrades & releases in line with the HMCTS testing requirements.	Met	

CST-SRVMGNT-046	Service Management	Testing	The Supplier shall conform to HMCTS testing documentation requirements, to ensure test plan(s) and report(s) are completed.	Met	
CST-SRVMGNT-047	Service Management	Information and Data	The Supplier, for the duration of the contract and agreed period thereafter, shall provide historical access to management information and service metrics as required by HMCTS in line with the HMCTS information and data standards.	Met	
CST-SRVMGNT-048	Service Management	Continual Improvement	The Supplier will provide Continuous Improvement (CI) and formal processes for HMCTS to request product improvements with feedback on the feasibility of the improvement and estimated release roadmap or version.	Met	
CST-SRVMGNT-049	Service Management	Disaster Recovery	The Supplier shall develop, maintain and provide an up-to-date Disaster Recovery Plans, developed in line with ISO27031 which are tested at least annually. The Supplier shall review/update the DR plan following live/test invocations and or significant changes to the functionality of the solution. Lessons learned must be tracked with improvement actions.	Met	
CST-SRVMGNT-050	Service Management	Disaster Recovery	The Supplier will ensure that after a Disaster Recovery (DR) scenario it is possible to recover the information associated with the solution to within a point in time agreed by the business of the time of failure. The solution must achieve a Recovery Point Objective (RPO) as set by HMCTS.	Met	
CST-SRVMGNT-051	Service Management	Disaster Recovery	The Supplier will ensure that after a Disaster Recovery (DR) scenario the supplier is able to recover the solution within the Recovery Time Objective (RTO) set by HMCTS.	Met	
CST-SRVMGNT-052	Service Management	Service Continuity	The Supplier shall proactively monitor the solution, identifying risks and proposing remediation actions that may impact on the continuity of service.	Met	
CST-SRVMGNT-053	Service Management	Service Continuity	The Supplier to ensure that their staff maintain full awareness of the stages within the Supplier's ITSCM Plan and be able to evidence this on request, through training records, test reports or equivalent.	Met	
CST-SRVMGNT-054	Service Management	Service Continuity	The Supplier shall develop, maintain and provide an up-to-date ITSCM Plan aligned to ISO27031, that is tested at least annually. The Supplier shall review/update the ITSCM plan following live/test invocations and or significant changes to the functionality of the solution.	Met	
CST-SRVMGNT-055	Service Management	Service Continuity	The Supplier should hold ISO/IEC 27031 certification and proactively maintain the skills and knowledge.	Not met	While Kerv does not have ISO 27031 certification, Kerv is currently working on obtaining ISO 22301 certification, which is a more extensive business continuity certification. Business continuity is currently

					audited under our ISO27001 certification.
CST-SRVMGNT-056	Service Management	Risk Management	The Supplier must have a risk management strategy and risk register which can be requested and reviewed by HMCTS.	Met	
CST-SRVMGNT-057	Service Management	Event Management	The Supplier will be expected to provide data, which can be used to gauge trending and other analytic reporting each <Day/Week/Month etc> for Events	Met	
CST-SRVMGNT-058	Service Management	Data migration	The Supplier should ensure facilitation of data migration from the buyers existing and future choice of solution.	Met	
CST-SRVMGNT-059	Service Management	Technical Management	The Supplier shall pro-actively monitor the ICT Environment to address actual or potential changes in performance characteristics and compliance with the agreed Service Levels.	Met	
CST-SRVMGNT-060	Service Management	Technical Management	The Supplier shall inform the Buyer within a required agreed notice period when there are any changes to software, in order to impact assess and mitigate any risks.	Met	
CST-SRVMGNT-061	Service Management	Technical Management	The Supplier must ensure that any equipment, hardware or software used in the provision of the solution will remain in service life support by the manufacturer for the Contract Period.	Met	
CST-SRVMGNT-062	Service Management	Technical Management	The Supplier must ensure that any software used in the provision of the solution that will be owned by the Buyer is available after the contract period in accordance with HMCTS data retention period.	Met	
CST-SRVMGNT-063	Service Management	Technical Management	The Supplier shall notify the Buyer within an agreed time when support for hardware, firmware or software used for the provision of the solution is to be withdrawn, to ensure that a review commences and that replacement deliverable(s) are identified, tested and made available before the manufacturer withdraws support.	Met	
CST-SRVMGNT-064	Service Management	Technical Management	The Supplier will ensure that upon discovery of non-compliance with the Open Standards, by any party, they will resolve the non-compliant state of the solution, or fully agree an exemption for non-compliance with the Buyer within 20 Working Days.	Met	

CST-SRVMGNT-065	Service Management	Collaboration	The Supplier shall co-operate with any other Supplier notified to the Supplier by the Buyer from time to time by providing: (i) reasonable information (including any Documentation); (ii) advice; and (iii) reasonable assistance, in connection with the solution to any such Other Supplier to enable such Other Supplier to create and maintain technical or organisational interfaces with the solution, to support design, delivery and integration of processes and solutions from multiple suppliers, to provide end to end support, and, on the expiry or termination of this Contract for any reason, to enable the timely transition of the solution (or any parts of this) to the Buyer and/or to any Replacement Supplier in accordance with the following collaborative working principles: a) Proactively leading on, mitigating and contributing to the resolution of problems, defects or issues irrespective of its contractual obligations, acting in accordance with the principle of "fix first, settle later"; b) Being open, transparent and responsive in sharing relevant and accurate information with such Other Suppliers; c) Where reasonable, adopting common working practices, terminology, standards and technology and a collaborative approach to solution development and resourcing with such Other Suppliers; d) Providing reasonable cooperation, support, information and assistance to such Other Suppliers in a proactive, transparent and open way and in a spirit of trust and mutual confidence; and e) Identifying, implementing and capitalising on opportunities to improve deliverables and deliver better solutions and performance throughout the relationship lifecycle.	Met	
CST-SRVMGNT-066	Service Management	Collaboration	The Supplier shall work with the Buyer and Other Suppliers in the development, implementation and operation of inter-supplier governance processes and meeting structures.	Met	
CST-SRVMGNT-067	Service Management	Collaboration	The Supplier shall escalate any issues with Other Suppliers, where the Supplier feels it is unable to resolve without intervention from the Buyer and or other suppliers in the Buyer's operating environment.	Met	
CST-SRVMGNT-068	Service Management	Collaboration	The Supplier shall provide technical account management as part of the service offering to support HMCTS maximise benefits of the solution.	Met	

Schedule 9 Service Level Schedule

[REDACTED]

Schedule 10 Call Traffic rate card

[REDACTED]

Schedule 11 – CX Email and CX Vizz End User Licence Agreement (“EULA”)

[REDACTED]