



Crown Commercial Service

G-Cloud 10 Call-Off Contract

This Call-Off Contract for the G-Cloud 10 Framework Agreement (RM1557.10) includes:

Part A - Order Form.....	1
Schedule 1 - Services	1
Schedule 2 - Call-Off Contract charges	1
Part B - Terms and conditions.....	1
Schedule 3 - Collaboration agreement	3
Schedule 4 - Alternative clauses.....	3
Schedule 5 - Guarantee	3
Schedule 6 - Glossary and interpretations.....	3
Schedule 7 - Processing, Personal Data and Data Subjects.....	4

Part A - Order Form


Digital Marketplace service ID number:	267479360522966
Call-Off Contract reference:	CQC ICTC 807
Call-Off Contract title:	Legal Case Management System
Call-Off Contract description:	The provision to supply and support a legal case Management System
Start date:	4 th April 2019
Expiry date:	3 rd April 2021
Call-Off Contract value:	<div style="background-color: black; width: 100%; height: 80px; margin-bottom: 5px;"></div> Total £136,800+ £8,000 + VAT = £173,760
Charging method:	Payment will be made in advance and on the anniversary date of the contract
Purchase order number:	TBC

This Order Form is issued under the G-Cloud 10 Framework Agreement (RM1557.10).




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

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

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

From: the Buyer	Care Quality Commission  Buyer's main address: 151 Buckingham Palace Road 3 rd Floor London SW1W 9SZ
To: the Supplier	Ilzuka Software Technologies Limited  Supplier's address: 2 Church Court Cox Street Birmingham B3 1RD Framework Company number: 4498601
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title:  Name:  Email: 
-----------------------	--

	Phone: [REDACTED]
For the Supplier:	Title: [REDACTED] Name: [REDACTED] Email: [REDACTED] Phone: [REDACTED]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 4 th April 2019 and is valid for 24 months
Ending (termination):	The notice period needed for Ending the Call-Off Contract is at least 60 working days from the date of written notice for undisputed sums or at least 30 working days from the date of written notice for ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 2 x 12 months period(s) by giving the Supplier 30 days written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud Lot:	This Call-Off Contract is for the provision of Services under: Lot 2 – Cloud software
---------------------	--

G-Cloud services required:	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> ● A deployment of Legal Case Management system that will address all the requirements CQC have requested within the requirements document covering functional business requirements and non-functional generic SaaS requirements. It adheres to the non- functional information security and architecture principals ● The advanced role engine will restrict access to data, workflows and information based on the agreed privileges of the user. Once logged in, a user will be presented with their relevant, timed workload and actions based on their progression through a case. ● The Supplier will provide a CQC configured version of Case Manager to CQC that will be determined by a series of requirements gathering workshops during implementation. ● The supplier will provide training to the configured Legal Case management system and provide support and ongoing maintenance during the contractual term of the call off contract
Additional services:	<p>The Buyer may request during the term of the contract additional services in relation to the scope of the primary service at a day rate to be agreed</p>
Location:	<p>The Solution will be delivered and will be accessible across the CQC infrastructure network. However, it is anticipated that services related to workshops and training time will need to be provided by the Supplier at the Buyer's Head Office (151 Buckingham Palace Road, London, SW1W 9SZ) and possibly at CQC other offices (i.e. Newcastle, Leeds) in order to understand, support and work with the Buyer's project team.</p>

Quality standards:	The quality standards required for this Call-Off Contract are ISO:27001 AND ISO:9001 AND CESH		
Technical standards:	The technical standards required for this Call-Off Contract are N/A		
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are		
	Indicator	Measured by	Review date/
	System availability	99.5% uptime	Quarterly
	Page response times	>2 seconds	Quarterly
	Indicator	Measured by	Review date/
	SLA Adherence	SLA Target met 100%	Quarterly
	Page response times	>2 seconds	Quarterly
Onboarding:	The onboarding plan for this Call-Off Contract is N/A.		
Offboarding:	The offboarding plan for this Call-Off Contract is The off-boarding plan for this Call-Off Contract is that upon Contract expiry the Supplier will be expected to provide the Buyer with access to all information gathered and produced as part of the delivery of the Services including the deliverables outlined in Table 1 of this Order Form (the majority of deliverables however should be received in-line with the dates outlined in Table 1). The off-boarding plan for this Call-Off Contract is Refer to Annex A supplier's response.		
Collaboration agreement:	N/A		
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £500,000.		
	The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-		

	<p>Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other defaults will not exceed the greater of £125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Insurance:	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> ● a minimum insurance period of [6 years] following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	<p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 15 consecutive days.</p>
Audit:	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits.</p>
Buyer's responsibilities:	<p>The Buyer is responsible for the granting of access to the Buyer's Head Office at 151 Buckingham Palace Road and any other Buyer premises required for the delivery of the Services. The Buyer is additionally responsible for ensuring the Supplier has access to the appropriate systems, materials and stakeholders required to deliver the deliverables outlined within this Order Form and Schedule 1 of this Agreement</p>
Buyer's equipment:	<p>The Buyer's equipment to be used with this Call-Off Contract includes.</p>

	It is anticipated that the Supplier will provide their own Computer equipment in order to conduct the services unless they request otherwise
--	--

Supplier's information

Subcontractors or partners:	The following is a list of the Supplier's Subcontractors or Partners Rackspace,
------------------------------------	--

Call-Off Contract charges and payment

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

Payment method:	The payment method for this Call-Off Contract is BACS
Payment profile:	The payment profile for this Call-Off Contract is annually
Invoice details:	The Supplier will issue electronic invoices annually. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to. T70 Payables F175, Phoenix House, Topcliffe Lane, Wakefield, West Yorkshire, WF3 1WE.
Invoice information required – for example purchase order, project reference:	All invoices must include. Purchase Order Number
Invoice frequency:	Invoice will be sent to the above invoice address.
Call-Off Contract value:	The total value of this Call-Off Contract is Total £136,800+ £8,000 + VAT = £173,760
Call-Off Contract charges:	The breakdown of the Charges is [REDACTED]

	<div style="background-color: black; width: 100%; height: 40px;"></div> <p>Total £136,800+ £8,000 + VAT = £173,760</p>
--	--

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones: N/A
Guarantee:	N/A
Warranties, representations:	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that N/A
Supplemental requirements in addition to the Call-Off terms:	Within the scope of the Call-Off Contract, the Supplier will N/A
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:	Within the scope of the Call-Off Contract, the Supplier will N/A
Public Services Network (PSN):	<p>The Public Services Network (PSN) is the Government's secure network.</p> <p>If the G-Cloud Services are to be delivered over PSN this should be detailed here: N/A</p>
Personal Data and Data Subjects:	Will Schedule 7 – Processing, Personal Data and Data Subjects be used Yes

1. Formation of contract

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

2. Background to the agreement

- (A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.10.
- (B) The Buyer provided an Order Form for Services to the Supplier.

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

Schedule 1 - Services

1. EXECUTIVE SUMMARY

- 1.1. The Care Quality Commission ("CQC") is a non-departmental public body established under the Health and Social Care Act 2008 ("HSCA 2008") and is the independent regulator of health and adult social care in England. Its purpose is to ensure that health and social care services provide people with safe, effective, compassionate, high-quality care and to encourage care services to improve.
- 1.2. CQC's Governance and Legal Services ("GLS") team provides appropriate internal controls, governance and legal support and advice, enabling CQC to fulfil its statutory duties under the HSCA 2008 and focus on achieving strategic objectives in an efficient and cost-effective manner.
- 1.3. Since April 2015 the CQC has had greater prosecution powers under the HSCA 2008 (Regulated Activities) Regulations 2014.
- 1.4. With an increase in enforcement activity and legal challenges as a result of the introduction of updated legislation, GLS is seeking to implement a legal case management system.
- 1.5. GLS currently has approximately 80 staff split over two groups. GLS staff is based in London, Leeds, Newcastle with some working remotely from home (please see Appendix 1).
- 1.6. GLS delivers expertise to internal clients by way of legal support and advice. It is split into the following sub-teams:
 1. Litigation, Prosecutions and Inquests Team;
 2. Adult Social Care Team;
 3. Primary Medical Services & Hospitals Team;
 5. Central Legal Services (incorporating the Advisory Team and the Commercial & Procurement Team);(See Appendix 2 for detailed description)
- 1.7. CQC sought a supplier to supply, install and support a software to assist management of cases within the GLS team, enabling it to deliver a more efficient and cost-effective service.
- 1.8. The new system was and remains necessary to enable delivery of an effective in house legal service that included courts and tribunal casework, efficient case progression, a directory of all internal and external contacts/stakeholders, letter and file review templates to enable GLS to fulfil recommendations following a Law Society compliance assessment.
- 1.9. It was and remains essential to have a legal case management system to meet the changing requirements of the functions and processes carried out by the GLS team and the objectives of our organisation.
- 1.10. Cases involving court deadlines and large volumes of disclosure continue to require effective management, in order to provide secure case delivery and compliance with judges' orders/directions. As part of its reform of the justice system and its efficiency programme, the government is investing in technology to improve the efficiency of court proceedings to allow for digital service and thus we need to reflect that drive.
- 1.11. The Legal team's work includes public and administrative law including the law in social care, health care and mental health; civil actions and criminal law; court and tribunal work; inquests; human rights; employment law; health and safety; property, contracts, procurement and information access.
- 1.12. In addition, we are under an obligation to ensure compliance with the Law Society and Solicitors Regulation Authority (SRA) Code of Conduct and Principles of working; as well as other legal regulatory bodies. We need to maintain a digital case management system without which we would not be able to have effective systems and controls in place to achieve and comply with the relevant principles, rules and outcomes and other requirements of the SRA Handbook.

2. SCOPE FOR LEGAL CASE MANAGEMENT SYSTEM

- 2.1. CQC needs to re-procure support and maintenance of the software system in accordance with the requirements stipulated in paragraph 3 below; including obtaining a licence as a service (a legal case management system) for initially two years with an option to extend for up to two further 12-month periods.
- 2.2. It is envisaged that the system will be licensed for approximately 65 users and training will be required as part of the implementation.
- 2.3. A continuous improvement plan to be implemented and delivery of priorities to be agreed by both parties.

3. THE REQUIREMENT

- 3.1. A case management enables legal cases to be better managed. It makes cases which are very high in volume of correspondence, emails and other documentation, and which have long life cycles, much more efficient to navigate and work with.
- 3.2. The GLS Team needs to be able to perform effectively in its role to support CQC as a regulatory body by using a case management system to carry out case supervision in accordance with the Law Society compliance guidance.

3.3. System Users

- Senior Management Team
- Legal Managers
- Senior Lawyers
- Lawyers
- Legal Officers
- Paralegals
- Legal

3.4. The main objectives remain for the GLS Team to accomplish the activities outlined below through the use of the Legal case management system:

- Accountability and collaborative working
- Workload management
- Complete audit trail for work where Legal Services are involved
- Time recording
- Content authoring
- Team capacity planning
- Management information reporting
- Introduction of new capabilities
- Digital case management
- Role based access control
- Collaborative working with external team resources
- Improving consistency and quality of service delivery
- Achieving deadlines or imposed dates
- Minimising risk
- Minimising duplication of data
- Document retention
- Enabling the service to grow to meet increasing demands for service

3.5. In order to continue to meet these key objectives, the following have been identified as key benefits and features of the Legal Case Management system and will provide the user with:

- A system capable of organising files and allowing for a quick and easy documents

access to legal advice, files, cases, information and data using a single interface

- A system that flags up deadlines by automatically adding them to the user's calendar
- Automated time recording
- A system capable of generating real time reports
- A self-service interactive system that allows users to know at a glance which Legal Advisor/Paralegal has conduct of a case and the status reporting
- Customized workflows for each practice area within legal services
- Formatted legal templates and precedents
- Automatically populates with key matter information.
- Electronically provides a link to electronic copies of documents and statutes
- Microsoft Office Integration emails
- Pagination, indexing and optical character recognition functions that will facilitate the preparation for trial bundles for use in court proceedings
- Remote access (when working from home)

3.6. Business Support

3.6.1. The solution should facilitate financial monitoring and budget management. It should be possible to design and run a number of reports to track financial performance/ expenditure (including disbursements and Counsel's fees) and allow forecasts to be made.

3.6.2. The solution should also allow suppliers to upload invoices directly to the system by way of for example a web-form, if those suppliers have already been provided with a purchase order number and a security code.

3.7. Training

3.7.1. The use of the system and training and development needs required to do so will be written in line with staff objectives. Meetings, workshops, training sessions, standard operating procedures etc. will be organised as required. We anticipate sessions to be facilitated by the supplier with training to be updated thereafter internally and/or externally as the needs of GLS develop together with the needs of CQC.

3.7.2. An impact assessment has been prepared which is available upon request.

3.7.3. A role specific training programme (to include an annual update/refreshers session) will be required for approximately 60 legal staff which includes Paralegals, Senior Lawyers; Lawyers and Legal Managers. Training to include an annual update/refreshers session.

3.7.4. Separate training programme on reporting, producing time reports, audit trails, case progression reports.

3.7.5. Separate training on how to create bespoke requests for information, re FOI requests and how to search the case management system to obtain this data.

4 LEGAL CASE MANAGEMENT SYSTEM – High Level and Functional Business Requirements

4.1 Suppliers to provide a solution that addresses the high level and functional business requirements.

4.2 Suppliers must address the high level functional, non-functional and security requirements in their response to the method statement of the evaluation criteria

4.3 As part of the evaluation process the functional business requirements will be assessed in line with the evaluation criteria.

Functional Business Requirements		
High Requirement	Level	Description – Functional Requirements
		<ul style="list-style-type: none"> • [SCM-1] As a Legal Adviser, I need the ability to collate information into a case so that all information related to a case can be accessed and recorded in a central place, thus increasing the effectiveness of the audit trail (i.e. collate all cases and organize information related to a specific case in individual folders such as witnesses, judges' orders, correspondence etc.) (MUST) • [SCM-36] As a Manager (All Sectors) I want to have the ability to allocate cases to legal Advisors so that cases are not duplicated, whilst also allocating the same case to a Paralegal (MUST) • [SCM-37] As a Legal Manager I want receipt acknowledgement for cases allocated so that I am certain that the case is being dealt with • [SCM-45] As a User I want the system to provide me with the ability to reallocate live cases where the allocated adviser may have left the team so that live cases are not left unallocated.(MUST) • [SCM-74] As a User, I need the ability to create documents with the contact details for the relevant persons automatically populated (i.e. Compile contact detail data related to case – regarding external solicitors, counsel, chambers, defense solicitors, witnesses and counsel – ensure letter produced automatically populate this information) • [SCM-39] As a Manager I want to have the ability to review the number of cases allocated to an Lawyer/Inspection Team so that cases are not over allocated • [SCM-40] As a User I want be able to view at glance the cases allocated to me, so that I can manage my caseload (MUST) • [SCM-47] As a System, I want to have the ability to link cases with each other if necessary, so that the I can see when multiple advises relate to a main case (Note: In Procurement it would be good to see when multiple advices relate to a main agreement) • [SCM-58] As a User I need to be able to save a document directly to a case so that document to be over-
	Workload Management	

	<p>seen by the manager is saved to the right case (MUST)</p> <ul style="list-style-type: none"> • [SCM-59] As a User, I want to have the ability to save documents in a single location with a clear chronology/dates with relevant subsection so that I do not have to waste valuable time looking for saved document (i.e. version control) (MUST) • [SCM-60] As a System, I want to have the ability to save documents in a single location with a clear chronology/dates with relevant subsection so that I do not have to waste valuable time looking for saved document (MUST) • [SCM-62] As a User, I want to have the ability to save email directly into a case file so that emails relating to the case can be accessed in-line with the case (MUST) • [SCM-63] As a System, I want emails to save automatically to the relevant folder within the case to which it's related in a chronological order, so that the user will be able to have the case history whenever they open the case • [SCM-38] As a Manager I want to have the ability to review the number of cases allocated to an advisor/officer/Inspection Team, so that cases are not over allocated (MUST) • [SCM-46] As a Manager (as well as all Users), I want to be able to view cases so that I can know the status of a particular case (MUST) • [SCM-48] As a User, I want the system to provide me with the ability to identify the adviser who worked on a document so that the team members are accountable • [SCM-7] As a Legal Adviser, I need the ability to prioritise cases within my allocated case load, so that I can effectively manage my workload • [SCM-41] As a Legal Adviser (Manager), I need the ability to request external Legal Advisors and allocate cases to them so that I am able to respond to peaks in demand for Legal Services team capacity and manage workload • As a Manager, I want to be able to review the completed and outstanding judges orders
Diary Management	<ul style="list-style-type: none"> • [SCM-50] As a System, I must have the ability to send alerts for tasks for which the due dates are set So that the User is reminded of the due dates e.g. warning notices. • [SCM-51] I want to receive alerts/prompts whenever I have to attend a court so that I do not miss court deadlines/criminal/civil procedure rules deadlines (MUST) • [SCM-75] As a user, I must have the ability to pull two or more cases together where there might be more than one enforcement action in progress at any given

	<p>time for a provider (For example, the case might involve fast track urgent action under s.31 but there is also slow track proceedings against the same provider. These cases can be merged under one case umbrella under the name of the Provider with a new ID or reference to incorporate both courses of action).</p>
Tasks, Templates and Prompts	<ul style="list-style-type: none"> • [SCM-12] As a Governance and Legal Services (GLS) Staff, I want a list of documents and observational prompts, specific to my sector and role so that <ol style="list-style-type: none"> a). I can readily see from the document list which sector it belongs to b). I can manage my case efficiently • [SCM-64] As a User I want to be able to pull up templates and precedents, so that I can use these at particular stages (MUST) • [SCM-65] As a User, I want to have access to templates, so that I can ensure that documentation/letters are consistent (i.e. dependent on the stage of proceeding – legal templates should be automatically populated to prompt. i.e. if I indicate a particular action on that case such as discontinuance I should be prompted to create a discontinuance letter. This letter will be automatically populated. This reminder should be sent to the allocated Lawyer and Paralegal) (MUST) • [SCM-66] As a User, I need the flexibility to be able to highlight important matters (i.e. color code cases) as high, medium and low priority so that I can manage the risk associated with the case (MUST) • [SCM-67] As a User, I want to have the flexibility to flag cases as high, medium or low risk (i.e. cases to have clear flags/alerts) so that I can know the risks associated with the cases e.g. cases that managers only can work on (MUST) •
Management Information Reporting	<ul style="list-style-type: none"> • [SCM-24] As a Legal Adviser, I need the ability to generate management information reports that provide information about the workload of the GLS teams so that GLS team capacity can be effectively managed. • [SCM-26] As a Legal Manager (Advisor) I need the ability to report on the present workload of internal and external Legal Advisors so that I can predict the future capacity needs of the team and only utilise external Legal Advisors where absolutely necessary thus operating in a cost-effective manner • [SCM-54] As a Case Progression Manager, I want to be able to provide accurate MI for reporting purposes; for GLS SLT, other Directorates/Teams, so that I can

	<p>respond to requests for information more easily and timely (i.e. information to be included in reports to are ET/CQC Board Members and its sub-committees. The benefit of having access to a variety of reports and to be also able to write bespoke reports. This is useful for requests for information and also as an SLT reporting and monitoring tool) (MUST)</p> <ul style="list-style-type: none"> • [SCM-29] As a Case Progression Manager (GLS), I need to be able to produce MI reports requested by External Stakeholders e.g. FOI, media, other Gov. Depts. etc. So that I can respond to requests for a variety of information more easily and timely. • [SCM-28] As a Case Progression Manager (GLS), I need to be able to produce PERFORMANCE reports for GLS SLT, So that I can respond to requests for a variety of PERFORMANCE REPORT more easily and timely. • [SCM-52] As a Manager/Admin I want to be able to obtain statistics for different activity types so that I do not have to manually go through workbooks to produce the required report. • [SCM-53] As a User, given that a case has being flagged as high, medium or low risks I want to have the ability to generate reports based on the risk rating of cases so that I know the number of High, Medium or Low Risks cases that I worked on in a given period e.g. weekly, monthly or yearly (i.e. A matter can be high risk due to commercial or political sensitivities for example, but that doesn't mean that the case is always the highest priority in terms of work load). • [SCM-25] As a GLS team lead I need to view other team members case work and identify trends or gaps to support a better way of working so that <ul style="list-style-type: none"> a). I can identify and respond to coaching requirements of team members, b). I can ascertain teams present capacity demands, c). I can provide internal quality assurance for the team
Manage cases- Search, Archive & Retrieve cases	<ul style="list-style-type: none"> • [SCM-19] As a Legal Services team member I need the ability to record advise given to Clients i.e. Inspector regarding a Provider so that at any point in the future, there is reliable audit trail of all information documented about the case in line with CQC legal responsibility • [SCM-70] As a User, I want to have the ability to search for cases e.g. previous cases, previous advice or conflict, so that I am able to cross reference my work to avoid duplicating work in order to manage my time efficiently (Note: search case by legislation, lawyer, court, tribunal, sector, provider) (MUST) • [SCM-68] As a User, I want to have the ability to archive cases, so that I can comply with legislation (MUST)

	<ul style="list-style-type: none"> • [SCM-69] As a User, I want to have the ability to retrieve archived case file so that I can look at cases related to cases that I am currently dealing with (MUST) • [SCM-21] As a Legal Adviser, I need an appropriate retention policy to be applied to the case when it is confirmed as complete so that we are compliant with our records management policy, and CQC can adhere to the Public Records Act 1958 and the General Data Protection Regulation (GDPR). • [SCM-72] As a User, I want to have the ability to retrieve files relating to the case I am working on so that I can continue working on it (MUST) • [SCM-73] As a User, I want to have the ability to retrieve information regarding cases/advice so that I can respond to freedom of information request (MUST)
Time Recording Cost & Fees	<ul style="list-style-type: none"> • [SCM-33] As a member of the legal team, I need to be able to record the time spent completing particular areas of legal work in order to submit a cost application to the court so that CQC can successfully recover cost incurred in providing legal services • [SCM-56] As a System, I want to have the ability to record the time spent by a case worker on a case so that the accurate time spent on the case is recorded for costing purposes (MUST) • [SCM-34] As a member of the legal team, I need to be able to record the time spent by external legal advisers in completing particular areas of legal work in order to verify the accuracy of fees application submitted to CQC So that CQC does not incur excessive fees • [SCM-32] As a legal Manager, I need to be able to assess the time spent on particular areas of work for succession planning so that I can allocate work more efficiently and for performance management • [SCM-49] As a User (all users), I need to be able to ensure cases/tasks are dealt with in specified time as per business protocol so that I know that I meet all deadline (MUST) • [SCM-57] As a User, I want to have the ability to record time spent on a case against given activities so that I know the total time spent on the case (For Example: If a case belongs to a given category or contract type, the user should be able to choose activity carried on the case from an activity list to show what task(s) they performed for the time spent) (MUST)
Digital Division of Labour	<ul style="list-style-type: none"> • [SCM-42] As a Legal Advisor (Manager) I need to assign sections of a case to different members of the Legal team (i.e. Paralegal, internal and external Legal Advisors), so that the relevant roles complete the appropriate sections and that we can work collaboratively and complete the case in good time • [SCM-43] As a User I want to be able to carry out

	conflict of interest search so that duplication can be avoided as well as avoid a joined up response across the sector (MUST)
Quality control feedback	<ul style="list-style-type: none"> • [SCM-23] As a member of GLS involved in the quality control of a case document I need to provide feedback to the author on a single source of the document so that <ul style="list-style-type: none"> a). good version control practices are adhered to b). an accurate audit trail is maintained in order see and refer to the historical development of a document

5 Non Functional Requirements

5.1 Suppliers to confirm that the tool being proposed is able to operate in line with the generic saas non-functional requirements.

5.2 As part of the evaluation process generic saas non-functional requirements will be assessed in line with the evaluation criteria.

Non Functional Requirements – Generic Software as a Service	
Availability requirements & support	
System availability	– Any system is required to meet service availability levels of 99.5% Monday to Friday 5 days a week with the exception of bank holidays. with system maintenance outside working hours
Required server environments	– The following server environments are required Live, Test, Development, User Acceptance Testing, Pre-production and Training, if appropriate to the nature of the service.
Disaster recovery	– System will be supported in the event of a disaster and any recovery plans will be tailored to CQC needs and be compliant with business continuity standards.
Recovery Time	
Recovery time & point objective	– The recovery mechanisms must support minimal recovery time with optimal recovery points.
Backup schedules	- Back-ups are to be carried out completely according to documented data back-up requirements. Appropriate personnel are to verify the usability of backed-up data and retain verification evidence.
Performance & scalability	
Storage	– The system must handle an increase in storage requirements without major system changes or data migration activities.
System scalability	- System shall be scalable both in terms of users and storage, with that easy to change both in terms of cost and minimal disruption.
Network performance and load	– The system must minimise the load on CQC's network and provide mechanisms for reporting on and controlling that load.
System performance	- Describe the typical response time that can be expected from an end user perspective when accessing the application, carrying out a typical task.
Integration	
Integration	– System must support authentication using CQC's existing active directory as part of its existing infrastructure managed service (Open Service) using ADFS.
Interface requirements	- Where relevant to its function, the system shall be capable of interfacing with CQC internal and external data sources, such as Siebel CRM, OBIEE, Oracle 11g, MySql, PostgreSQL and SQLServer 2008 and aboveAs stated in the Architecture Principles, a service oriented approach should be used, where practical and possible.
Use of mobile devices	- System shall support the use of a range of mobile devices, meeting CESG requirements.
Monitoring	
Application monitoring	- The application must be monitored by the provider, with suitable alerting tools in place to notify of current or imminent service breaches and security issues.
Reporting	
Availability reporting	- Provide examples of daily, weekly and monthly application availability reporting.

Capacity reporting - provide examples of monthly reporting on current versus projected capacity, both in terms of storage and licenses.
Service Management reporting - provide examples of daily, weekly and monthly reporting on the overall performance on the service, including performance, requests and incidents relating to the service.
Change management and release process
Change management - Demonstrate your ability to perform changes to the application in a controlled and structured manner, including adherence to any methodologies.
Release Management - System to be subject to formal processes for release management, in association with customer with regard to testing.
Segregation of environments - Responsibilities related to program coding, application testing and approval, program transfer between environments are segregated
Usability
Language support - The application must support UK English.
Desktop support - All system configuration settings are remotely accessible to the system administrator through application screens or setup programs (i.e. no hard coded system variables exist and include system, user, roles, company and other configuration screens).
User experience – The solution must provide an intuitive user interface that enables the user to complete a task whilst minimising the need to navigate the system
Software as service - Customer Desktop devices are restricted in terms of the ability to download components from external sources. The system shall operate with the minimal need for software components to be applied to PC or desktop devices. The CQC standard desktop is Windows 10 64 bit with Internet Explorer 10 and integration with Exchange online and Microsoft Office 365. The supplier must provide comprehensive systems administration, installation guides and processes, as appropriate to the nature of the service. A complete, typical deployment architecture must be described.
Compliance
Open service IT standards - The application must comply with the CQC Architecture Principles.
Legal compliance - Compliance to all U.K. legal requirements including the General Data Protection Regulation (GDPR), the Freedom of Information Act (2001) & Privacy laws.
Government Technology Strategies – The system or service must comply with the U.K. Government Digital strategy
Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.
Escrow
Source code availability - In the event of buyout or liquidation of the vendor the base source code of the software must be made available to CQC.
Support
Service desk & service manager - Supplier shall provide a service desk with the ability to log and resolve incidents and requests. The supplier shall provide a named contact for escalation of issues and regular interface between the supplier and the customer. The supplier shall detail the channels available and typical response times for both fault resolution and functional query support.
Accessibility
Accessibility – The system shall enable accessibility via assistive technology

gy for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Speak and Windows 10 Voice Recognition software. It shall also enable access for those with additional visual or hearing needs. The supplier shall state how these needs are met by the software.

6. Non Functional Requirements – Information Security

6.1 Suppliers to confirm that the tool being proposed is able to operate in line with the information security non-functional requirements.

6.2 As part of the evaluation process the information security non-functional requirements will be assessed in line with the evaluation criteria.

Non Functional Requirements – Information Security	
Session security	
Login	All user identifiers must be linked to roles which have explicit and granular assignments to access levels that enforce a restriction on the ability of the end user to create, read, update and delete information.
Password requirements	Passwords must be configurable and enable enforcement to have a minimum length of 8 characters with a mixture of lower and upper case characters and symbols, as required by CQC policies which may vary between devices. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.
Password requirements for administrator accounts	Passwords for administrator accounts must be configurable and enable enforcement to have a minimum length of 10 characters with a mixture of lower and upper case characters and symbols. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.
Inactivity timeout	Where the solution maintains a user session, it must be able to configured to timeout as needed for the particular use case.
Identity	
Client applications	The solution will identify all client applications before allowing them to use its capabilities.
End users	The solution will identify all of its human users before allowing them to use its capabilities.
Physical access	All personnel will be required to present relevant identification before they are allowed access to secure locations such as CQC offices or data centres.
Single sign on	The solution will not require an individual user to identify themselves multiple times during a session (single sign on).
Inactivity	The solution must provide a mechanism for suspending user accounts when they have not been used for a predefined period.
Employee status	The supplier must prevent access to customer data and systems by employees who are leaving its employment and disclose their policy and procedures regarding this.
Authentication	
Access to capabilities	The solution will authenticate all users before allowing them to use its capabilities.
Access to user details	The solution will authenticate of all users before allowing them to update their user information.
Access by client applications	The solution will authenticate all client applications before allowing them to use its capabilities. It should be capable of interfacing with Azure Active Directory.
Authorisation	
Own personal information	The solution will allow each user to access to

all of their own personal information, where applicable.
Others personal information – The solution will only allow users access to the personal information of other users, where a business case for that exists.
Access restrictions – The solution will be capable of restricting access to specified areas or databases.
Password repository – The solution will not allow access to the user password or hash database / file.
Incorrect credentials – The solution will create increasing time periods between the entry of incorrect credentials in order to prevent brute force passwords or denial of service attacks.
Immunity (AV) and
Threat identification - The solution will protect itself from infection by scanning all entered or downloaded data and software for known computer viruses, worms, Trojans and other similar harmful programs.
Threat removal - The solution will be capable of disinfecting or quarantining any file found to contain harmful programs.
Threat alerting - The solution will alert an administrator of any harmful software found during scans.
Threat currency - The solution will regularly (daily or weekly) update the anti-virus definition files.
Innovation – Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.
Intrusion Detection and Protection
Authentication failure – The solution will detect, prevent and record all access attempts which fail identification, authentication or authorisation requirements.
Intrusion notification - The solution will be capable of reporting on all failed access. The application will notify the administrator(s) within 5 minutes of the IPS system triggering alerts.
Innovation – Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.
Physical Access – Where connectivity is provided to end point devices network access controls must be in place to ensure that only authorised and secured endpoints are able to access network resources.
Audit
Audited elements - The business elements that will be audited must be stated explicitly.
Audited fields – The data fields that will be audited must be stated explicitly.
Audit logs – The audit logs should be configurable to record activities appropriate to the system.
Enhanced privileges – A record of all activity by accounts with enhanced privileges must be retained for three months.
Audit status - The solution will collect, organise, summarise and regularly report the status of its security mechanisms.
Security
Data – The solution must include security measures and controls suitable for holding data up to and including OFFICIAL SENSITIVE, where required.
Disposal – The solution must provide for the secure deletion of any information held on behalf of the customer as the result of the disposal of equipment or change or cessation of the service.
Patching – CQC must be notified when patches or fixes are released for the solution and provided a means to access and apply at short notice any urgent patches resulting from a security exposure. Patching support must be

continued for old versions of the software and must be continued for a minimum of two years after the release of a major version that supersedes the prior version. This must be included as part of the support and maintenance costs. The solution should follow the 'evergreen' strategy for patching.

Credentials – The solution must not persist its own user credentials at the presentation or application layer and not persist any external credentials except through the use of tokens.

Authentication and access – The solution shall support 1 user account per user. The service shall be demonstrably capable of segregating access to functions and data based on roles for specific users. This must include the ability to control access to create, read, update and delete functions acting on the data objects managed by the software.

Identity & access management

Formal approval of user changes – the solution must provide an audit trail of all user account and access management actions such as creating, amending and removing.

Account lock out - The number of failed login attempts before system lock-out is 5 attempts or less and this value is able to be configured by an administrator.

Database access restrictions - For solutions that have a separate database, such as SqlServer or Oracle, access to the database must be able to be restricted to appropriate and authorised personnel only. For solutions that have a separate database, database accounts and their roles/groups are reviewed periodically for appropriateness. The solution must not use hard coded identifiers or passwords to connect to the database.

Integrity

Integrity - The solution will maintain the integrity of data and have appropriate controls and segregation of access to securely manage data throughout the data lifecycle.

Audit of use – The solution must demonstrate the ability to be configured to generate an accessible log of users' access to data for Create, Read, Update and Delete.

Non-Repudiation

Non-repudiation - The solution will securely segregate and store all data (logs) relating to user actions on the system(s) including:

- Actions carried out i.e. read, write, change
- Date and time actions were carried out
- The identity of the user by unique credentials

Compliance

Legal compliance - Compliance to all U.K. legal requirements including the General Data Protection Regulation (GDPR), the Freedom of Information Act (2001) & Privacy laws.

Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.

Escrow

Source code availability - In the event of buyout or liquidation of the vendor the base source code of the solution must be made available to CQC.

Data centre

Physical damage - The data centre will protect its hardware components from physical damage, destruction, theft or surreptitious replacement.

Hosting – The system must be hosted by an ISO27001 accredited organisation and must also be demonstrably capable of holding data up to and including OFFICIAL SENSITIVE. Patching must take place in line with the

software manufacturer's recommendations and be able to be applied at short notice in the event of a security exposure being identified. This must be included as part of the support and maintenance costs.
Death and injury - The data centre will protect staff from death and injury.
Physical application access - The application will be protected against unauthorised physical access.
Maintenance
System maintenance – System maintenance will not violate any of the security requirements as a result of upgrades or replacement of hardware, software or data.
Additional cloud services requirements
Data ownership - All data remains the property of CQC and may not be used by the contractor except for processing as directed by CQC.
Documentation
Required documentation – The implementation of each security requirement must be documented and approved by named individuals and distributed on an explicit and controlled circulation.

7. Billing Module Requirements

Billing Module to be agreed

Annex A - Supplier Response to Functional Requirements

Overview

IIZUKA proposes to implement a solution to the CQC LCMS requirements based on its proven Case Manager platform. Case Manager is not a specialised Legal Case Management system, but is a highly configurable, enterprise level case management platform that is used by a wide range of organisations across the UK public and third sectors for a wide range of case management purposes. Case Manager is deployed as a securely hosted, managed service platform that is then configured to meet the exact needs of the customer depending on their types of case, established working practices, security and management information requirements.

IIZUKA has a proven track record of delivering reliable, mission critical and highly secure systems to organisations such as the Foreign & Commonwealth Office, the Pensions Ombudsman and numerous local authorities, advice agencies, emergency services, housing associations, industry bodies and more.

IIZUKA provides the service by working closely with the customer in the early stages of implementation to understand the business requirements in detail and then to configure the Case Manager system appropriately. This configuration is done within the system itself and can be gradually handed over to authorised and trained users within the CQC, so that future changes in legislation, organisational direction or business practices can be easily accounted for; resulting in a truly future proof solution.

Below, we have provided responses to the stated requirements with references, where relevant, to some example screens from a Case Manager system that has been configured with an outline structure that meets the needs of the CQC.

IIZUKA Response to LCMS Requirements ITT

Screenshot 1 – Case Screen

The screen below shows an example case screen, including linked records for witnesses and case contacts, actions that are available to be assigned in relation to this case and the chronological case action history, including two actions that are still outstanding but within their scheduled dates.



Steve Randerson | Sign Out

V: 1.2.1.1 | Support | Home | New Case | Search | Reports

Your Location: Home > Client > Case

Case Tasks

[Edit details](#)
[Reassign](#)
[Change type](#)
[Add note](#)
[Add follow-up](#)
[Link to another case](#)
[Set responsibilities](#)
[Record time spent](#)
[Set involvement](#)

Status Tasks

[Close](#)
[Progress Casework](#)
[Document Tasks](#)
[Generate document](#)
[Messaging Tasks](#)
[Send Message](#)

Case Details

Summary

CA-RDCWFW

24/01/2017 15:04

New Enquiry

Steve Randerson

Owner

Steve Randerson

Responsibilities

Division Maker

Case Contact

Witness

Description

Partnership

Reference

12/02/1986

10 Any Street, Anytown, ME1 1RE

Flags

Available Actions

Book an appointment for the client

Client

Care Quality Commission

Duration: 30 (mins)

Add

Schedule a general task or case action

General task

Care Quality Commission

Add

Refer the case to another agency

Refer

Make Referral

Suggest the client or make the referral directly as appropriate

Add

Assign a task to the current paralegal for this case

Paralegal task

Paralegal task

Add

Contact

Courts

Case Action	Time Records	Correspondence	Letters	Linked Cases	Guidance	Security
<div> <div>Status</div> <div> <div>Acknowledged</div> <div>23/02/2017 10:00</div> <div>Appointment</div> </div> </div>	<div> <div>Summary</div> <div>Court Hearing</div> <div>23/02/2017 10:00-10:45</div> </div>	<div> <div>Owner</div> <div>Steve Randerson (Care Quality Commission)</div> </div>				
<div> <div>Requested</div> <div>29/01/2017 21:07</div> <div>Task</div> </div>	<div> <div>Paralegal Task</div> <div>Validity Check</div> </div>	<div> <div>Owner</div> <div>Helen Parker (Care Quality Commission)</div> </div>				
<div> <div>Complete</div> <div>24/01/2017 21:05</div> <div>Note</div> </div>	<div> <div>Initial thoughts</div> </div>	<div> <div>Owner</div> <div>Steve Randerson (Care Quality Commission)</div> </div>				
<div> <div>Complete</div> <div>24/01/2017 21:04</div> <div>Immediate Resolution</div> </div>	<div> <div>Contact Out</div> </div>	<div> <div>Owner</div> <div>Steve Randerson (Care Quality Commission)</div> </div>				
<div> <div>Complete</div> <div>24/01/2017 21:04</div> <div>Immediate Resolution</div> </div>	<div> <div>Contact in</div> </div>	<div> <div>Owner</div> <div>Steve Randerson (Care Quality Commission)</div> </div>				
<div> <div>Complete</div> <div>24/01/2017 15:04</div> <div>Opening Contact</div> </div>	<div> <div>Telephone</div> </div>	<div> <div>Owner</div> <div>Steve Randerson (Care Quality Commission)</div> </div>				

Screenshot 2 - Management Dashboard

The screenshot below shows an example management dashboard that displays a chart of the case allocation with the logged in user's team and a filterable list of the cases that are currently open across the team.

My Cases

My Case Actions

Calendar

My Team's Cases

My Team's Case Actions

Team

Time Tasks

Record time spent

My time records

My Profile

My details

Change password

Manage dashboards

Dashboard

My Team's Caseload

Paula Jones

Case Owner: 2

Claire Beckett

Paula Jones

Steve Randerson

My Team Members' Cases

Status	Open Date	Client	Reference	Type	Owner	Summary
New Enquiry	24/01/2017 15:04	Fred Bloggs	CA-RDCWFW	CQC: Adult Social Care	Steve Randerson	
New Enquiry	24/01/2017 21:19	Keand Winter	CA-RDCWHY	CQC: Adult Social Care	Paula Jones	
New Enquiry	24/01/2017 21:20	Frank Vincent	CA-RDCWCS	CQC: Adult Social Care	Claire Beckett	
In Progress	24/01/2017 21:19	Derek Shabier	CA-RDCWNZ	CQC: Adult Social Care	Paula Jones	
New Enquiry	24/01/2017 21:33	Eric Handley	CA-RDCWBR	CQC: Primary Medical Services, Hospitals and Registration	Steve Randerson	

Previous

Next

Showing 1 to 5 of 5 entries

Show 10 entries

Team

My Team's Caseload

Claire Beckett

Paula Jones

Case Owner: 2

Claire Beckett

Paula Jones

Steve Randerson

My Team Members' Cases

Status	Open Date	Client	Reference	Type	Owner	Summary
New Enquiry	24/01/2017 15:04	Fred Bloggs	CA-RDCWFW	CQC: Adult Social Care	Steve Randerson	
New Enquiry	24/01/2017 21:19	Keand Winter	CA-RDCWHY	CQC: Adult Social Care	Paula Jones	
New Enquiry	24/01/2017 21:20	Frank Vincent	CA-RDCWCS	CQC: Adult Social Care	Claire Beckett	
In Progress	24/01/2017 21:19	Derek Shabier	CA-RDCWNZ	CQC: Adult Social Care	Paula Jones	
New Enquiry	24/01/2017 21:33	Eric Handley	CA-RDCWBR	CQC: Primary Medical Services, Hospitals and Registration	Steve Randerson	

Previous

Next

Showing 1 to 5 of 5 entries

Show 10 entries

Dashboard

My Team's Caseload

Paula Jones

Case Owner: 2

Claire Beckett

Paula Jones

Steve Randerson

IIZUKA Response to LCMS Requirements ITT

Functional Business Requirements

Functional Requirements

Response

Workload Management

[SCM-1] As a Legal Adviser, I need the ability to collate information into a case so that all information related to a case can be accessed and recorded in a central place, thus increasing the effectiveness of the audit trail (i.e. collate all cases and organize information related to a specific case in individual folders such as witnesses, judges' orders, correspondence etc.) (MUST)

Case Manager is a case management system with a strong and flexible information architecture that allows the case to be recorded and structured records to be linked to the case or included within it. Structured records within the case can be a wide range of things, including people, documents, notes, tasks and actions and many more.

Case Manager provides access to all of this from a single, easily navigable place. Screenshot 1 above shows a sample case screen with various elements displayed and links to other areas easily accessible so that users can quickly navigate to the relevant pieces of information.

A key feature of Case Manager is a configurable 'View' system where customised views of a case can be created that provide specialised displays of the information within a case for different users or different purposes. Examples include summary views, full disclosure views and 3rd party views.

[SCM-36] As a Manager (All Sectors) I want to have the ability to allocate cases to legal Advisors so that cases are not duplicated , whilst also allocating the same case to a paralegal (MUST)

Case Manager provides a wide range of tools for managing the assignment of cases themselves or actions within cases to organisations, teams or individuals. Assignments can be made by authorised users and can be tracked and managed from within the case records.

Dashboards are provided that give managers immediate visibility of current allocation levels, with options to 'drill down' or filter dashboards so that specific aspects of allocation can be viewed and managed.

Case Manager has a fully configurable workflow and action assignment system that allows both the case and actions within it to be assigned separately. This allows multiple people to be

IIZUKA Response to LCMS Requirements ITT

	involved in a case; each with their own tasks and responsibilities. For example a case can be assigned to one owner as the overall manager, with another being identified as the paralegal for the case. Other users can easily identify these people when viewing the case and relevant actions can be automatically assigned to them based on their relationship to the case.
[SCM-37] As a Legal Manager I want receipt acknowledgement for cases allocated so that I am certain that the case is being dealt with	Case Manager provides a workflow around assignment that tracks when actions or cases are assigned, when or if they have been acknowledged and whether they have been completed or not. Users can be notified automatically when actions are progressed or near or pass a deadline. The status of actions is also clearly displayed within a case, so that users working with the case can easily see what other actions are outstanding, by when and by whom. Dashboards are also provided that that allow users and their managers to see the actions they are currently assigned, in line with prioritisation and due dates.
[SCM-45] As a User I want the system to provide me with the ability to reallocate live cases where the allocated adviser may have left the team so that live cases are not left unallocated.(MUST)	Case Manager allows cases to be accessed by users other than the owner (subject to access control permissions) and re-allocated. Actions can also be picked up by other team members, in the case of short term absence. Where actions are outstanding, they are tracked and made clearly visible to managers and other team members, ensuring that cases awaiting action are not lost when the users primarily responsible for them are not available or no longer in post.
[SCM-74] As a User, I need the ability to create documents with the contact details for the relevant persons automatically populated (i.e. Compile contact detail data related to case – regarding external solicitors, counsel, chambers, defense solicitors, witnesses and counsel – ensure letter produced automatically populate this information)	Case Manager includes a document generation module that allows letters, documents and forms to be generated from within case records, or other linked records, with details such as names, dates, notes, addresses and contact details and more automatically populated.

IIZUKA Response to LCMS Requirements ITT

<p>[SCM-44] As a User, Given that a complaint has being raised; And the case has being allocated to me; I want to have the ability to review the complaint so that I can review the right complaints based on the following criteria (i.e. Provide legal advice in a specified template – include prompts for sections on evidential test and public interest test) (MUST)</p>	<p>Users can view cases assigned to them and can access all of the case information and see the full history of the case, subject to having sufficient authorisation levels. Case Manager includes a fully configurable workflow, field and action management system, plus a document generation system. In combination, these can be configured to provide the prompts relevant to the CQC business processes. During the early implementation phase of the project IIZUKA will work with the CQC through workshop, requirements gathering sessions or work shadowing to determine the processes that are needed and will assist the CQC in configuring the system to exactly meet the business' needs.</p>
<p>[SCM-39] As a Manager I want to have the ability to review the number of cases allocated to an advisor/officer/Inspection Team so that cases are not over allocated</p>	<p>Case Manager allows users to track the number of cases and actions assigned to users, teams and 3rd party organisations. This information is available in management information reports and in dynamic dashboards that support both filterable tables and graphical charts, with drill down. Screenshot 2 above shows an example dashboard giving management oversight of allocation levels within a team.</p>
<p>[SCM-40] As a User I want be able to view at glance the cases allocated to me, so that I can manage my caseload (MUST)</p>	<p>Case Manager provides users with a personalised dashboard that gives them immediate access to cases that are relevant to them. This includes a list of all cases assigned to the user. Users can also access lists of cases assigned to other people in their team, so that they can provide cover during staff absences.</p>
<p>[SCM-47] As a System, I want to have the ability to link cases with each other if necessary, so that the I can see when multiple advises relate to a main case (Note: In Procurement it would be good to see when multiple advices relate to a main agreement)</p>	<p>Case Manager allows cases to be linked through named types of links. Authorised administrators can defined the types of link available for use, with examples including related cases, duplicate cases, parent cases, master cases and more. During the implementation phase of the project IIZUKA will analyse the requirement in more detail and assist in the configuration of appropriate link types and workflow. When cases are linked, the links can be easily seen by users</p>

IIZUKA Response to LCMS Requirements ITT

	when looking at each case and can be followed to take the user to the relevant linked record.
[SCM-58] As a User I need to be able to save a document directly to a case so that document to be overseen by the manager is saved to the right case (MUST)	Case Manager allows users to attach files, including documents, to cases. Documents are uploaded to the system and held securely as part of the case record, protected by the same security rules that govern access to the case itself. After documents are attached then there is no need for copies to be held in shared drives, users are then able to retrieve documents by downloading them from the case record. This is supported even if the user is out of the office, provided that they are able to access the system online or are using the offline synchronised mobile application.
[SCM-59] As a User, I want to have the ability to save documents in a single location with a clear chronology/dates with relevant subsection so that I do not have to waste valuable time looking for saved document (i.e. version control) (MUST)	Documents attached to cases in Case Manager are easily accessible from the case record to which they are attached. They can be accessed in chronological order. Version control is not a standard Case Manager feature, but is available as an additional module if required. IIZUKA will assess the detailed requirements for document management during the requirements analysis phase of the project, and determine the configuration and modules required.
[SCM-60] As a System, I want to have the ability to save documents in a single location with a clear chronology/dates with relevant subsection so that I do not have to waste valuable time looking for saved document (MUST)	As per requirement SCM-59 above, Case Manager supports the attachment of documents to a Case and presents them for access in Chronological order.
[SCM-61] As a Member of the Complaints Team, I want to be able to save background of case so that I know what the case is about (MUST)	Case Manager allows users to record notes and other structured records within a case. The system can be configured to provide the fields necessary for recording the details of the different types of CQC cases, this can include long text fields, allowing for long notes and background information, or specific field types such as dates, statuses, pick lists and many more. IIZUKA will assess the detailed requirements for the different types of CQC cases during the

IIZUKA Response to LCMS Requirements ITT

	requirements analysis phase of the project and determine the appropriate configuration required.
[SCM-62] As a User, I want to have the ability to save email directly into a case file so that emails relating to the case can be accessed in-line with the case (MUST)	Case Manager allows the text from emails to be copied and pasted into notes fields, or for the emails to be saved as files and uploaded to the case as attachments. IIZUKA will investigate the CQC operating environment and advise on the best approach and configuration to use for this requirement. Regardless of the option chosen, the emails can be accessed by users via the case record.
[SCM-63] As a System, I want emails to save automatically to the relevant folder within the case to which it's related in a chronological order, so that the user will be able to have the case history whenever they open the case	Attachments and other actions saved to cases within Case Manager are accessible in chronological order from the Case Actions display of the case.
[SCM-38] As a Manager I want to have the ability to review the number of cases allocated to an advisor/officer/Inspection Team, so that cases are not over allocated (MUST)	Case Manager tracks the assignment and status of each case and provides management information dashboards and reports that allow managers to easily see the levels of allocation. Allocation can be viewed at the individual, team or organisation level.
[SCM-46] As a Manager (as well as all Users), I want to be able to view cases so that I can know the status of a particular case (MUST)	Case Manager has a fully configurable workflow system that allows cases to move through a workflow that is specific to the type of case. The status of the case is clearly displayed within the case and in dashboards, reports and views where the case appears. IIZUKA will assess the workflows required by the CQC as part of the requirements analysis phase and determine the appropriate configuration for the system.
[SCM-48] As a User, I want the system to provide me with the ability to identify the adviser who worked on a document so that the team members are accountable	Case Manager includes a full audit trail of every action performed, including the action that was done, the user that did it and the date and time. This applies to cases, documents and all other record types in the system. Key status, action and ownership information is also recorded for major types of records for easy display from within the main case record, without the need for users to access the detailed audit logs.

IIZUKA Response to LCMS Requirements ITT

<p>[SCM-7] As a Legal Adviser, I need the ability to prioritize cases within my allocated case load, so that I can effectively manage my workload</p>	<p>Case Manager supports both automatic and manual prioritisation of workload. Automatic prioritisation is based on the due dates of scheduled actions, with more immediate actions automatically prioritised above those that are due later. Manual prioritisation allows users to set the priority of an action or case. Work queues are provided through the user's personalised dashboards that display the outstanding work in priority order.</p>
<p>[SCM-41] As a Legal Adviser (Manager), I need the ability to request external Legal Advisors and allocate cases to them so that I am able to respond to peaks in demand for Legal Services team capacity and manage workload</p>	<p>Case Manager provides a wide range of options for working with external agencies and third parties. As a hosted system, accessible via the Internet, external agencies can be granted direct access to the system to receive allocations, access their own work queues and log actions completed against cases. Where this is not possible because of practical, commercial or security considerations there are options for logging actions on behalf of external agencies, provision of a simplified access portal or for direct integration with external provider's systems. This requirement (SCM-41) provides insufficient detail to be able to determine the best solution to this requirement at this stage, so IIZUKA will assess the requirement in more detail during the implementation phase and determine which of the available options best meets the requirement. IIZUKA reserves the right to alter the pricing depending on the option chosen.</p>
<p>As a Manager, I want to be able to review the completed and outstanding judges orders</p>	<p>Judges Orders will be configured within the system as part of the case and action workflow and made available to managers through dashboards and reports. They will also be accessible from within the related case record.</p>
<p>Diary Management [SCM-50] As a System, I must have the ability to send alerts for tasks for which the due dates are set So that the User is reminded of the due dates e.g. warning notices.</p>	<p>Case Manager automatically notifies users via email in a range of situations. This includes when they are assigned a new action or case, when a warning period on a due date is reached or when the due date itself is reached. Notifications contain a link that takes the user directly to the case or action in the system so that they can see the details or</p>

IIZUKA Response to LCMS Requirements ITT

<p>[SCM-51] I want to receive alerts/prompts whenever I have to attend a court so that I do not miss court deadlines/criminal/civil procedure rules deadlines (MUST)</p>	<p>make updates as required.</p> <p>Deadlines can be scheduled as action dates within a case, either automatically based on rules or manually by users. Those actions are then tracked by the system and alerts sent to users when the actions have not been completed or the warning threshold is reached.</p>
<p>[SCM-75] As a user, I must have the ability to pull two or more cases together where there might be more than one enforcement action in progress at any given time for a provider (For example, the case might involve fast track urgent action under s.31 but there is also slow track proceedings against the same provider. These cases can be merged under one case umbrella under the name of the Provider with a new ID or reference to incorporate both courses of action).</p>	<p>Case Manager allows cases to be linked together, but still retain separate time scales, status and histories and also for individual cases to have multiple streams of activity, again with separate allocation, status and timescales. These features allow scenarios such as that described to be modelled and followed easily within the system.</p>
<p>Tasks, Templates and Prompts</p> <p>[SCM-12] As a Governance and Legal Services (GLS) Staff, I want a list of documents and observational prompts, specific to my sector and role so that</p> <p>a). I can readily see from the document list which sector it belongs to</p> <p>b). I can manage my case efficiently</p>	<p>Case Manager allows for configurable document templates, prompts and actions dependent on the role of the user and the type of the case (amongst other things), so these features can be used to provide GLS staff with a tool that is specific to their role. The specific configuration required will be determined during the requirements analysis phase of the project.</p>
<p>[SCM-64] As a User I want to be able to pull up templates and precedents, so that I can use these at particular stages (MUST)</p>	<p>Case Manage supports the use of document templates that allow for the automatic generation of documents, with key details automatically populated by information from within the case record. Document templates can be configured using filters so that they appear only when relevant to the particular case and its current status. This allows the user to benefit from access to templates, but without requiring them to hunt through large volumes of templates to find the relevant action. Once a template is selected and the document generated,</p>

IIZUKA Response to LCMS Requirements ITT

<p>[SCM-65] As a User, I want to have access to templates, so that I can ensure that documentation/letters are consistent (i.e. dependent on the stage of proceeding – legal templates should be automatically populated to prompt. i.e. if I indicate a particular action on that case such as discontinuance I should be prompted to create a discontinuance letter. This letter will be automatically populated. This reminder should be sent to the allocated lawyer and Paralegal) (MUST)</p>	<p>users can make amendments to the document before it is finalised, published and made a permanent part of the case record.</p> <p>Case Manager supports configurable work flows that allow the generation of actions to relevant staff and to generate documents from templates that automatically include relevant information from the case. Templates are configured with rules that make them available only at the point in a case workflow where they are relevant.</p>
<p>[SCM-66] As a User, I need the flexibility to be able to highlight important matters(i.e. color code cases) as high, medium and low priority so that I can manage the risk associated with the case (MUST)</p>	<p>Case Manager allows cases to be flagged with priority, risk or other categorisation and for these flags to be automatically highlighted when viewing cases or their action in dashboards and work queues.</p>
<p>[SCM-67] As a User, I want to have the flexibility to flag cases as high, medium or low risk (i.e. cases to have clear flags/alerts) so that I can know the risks associated with the cases e.g. Cases that managers only can work on (MUST)</p>	<p>Case Manager allows cases to be flagged with a risk and for them to be moved through the workflow so that only managers can work on them.</p>
<p>Management Information Reporting</p> <p>[SCM-24] As a Legal Adviser, I need the ability to generate management information reports that provide information about the workload of the GLS teams so that GLS team capacity can be effectively managed.</p>	<p>Case Manager automatically tracks the cases and actions allocated to individuals, teams and organisations and allows users to see the amount of work allocated through management information reports and dynamic dashboards. Screenshot 2 above shows an example dashboard where the number of cases allocated to staff can be seen.</p>
<p>[SCM-26] As a Legal Manager (Advisor) I need the ability to report on the present workload of internal and external Legal Advisors so that I can predict the future capacity needs of the</p>	<p>Case Manager allows the workload of all types of user or external party to be managed and viewed so that users can make appropriate resourcing and capacity decisions.</p>

IIZUKA Response to LCMS Requirements ITT

team and only utilize external Legal Advisors where absolutely necessary thus operating in a cost effective manner

[SCM-54] As a Business Manager, I want to be able to provide accurate MI for reporting purposes; for GLS SMT, other Directorates/Teams, so that I can respond to requests for information more easily and timely (i.e. information to be included in reports to are ET/CQC Board Members and its sub-committees. The benefit of having access to a variety of reports and to be also able to write bespoke reports. This is useful for requests for information and also as an SMT reporting and monitoring tool) (MUST)

[SCM-29] As a Business Manager (GLS), I need to be able to produce MI reports requested by External Stakeholders e.g. FOI, media, other Gov. Depts. etc. So that I can respond to requests for a variety of information more easily and timely.

[SCM-28] As a Business Manager (GLS), I need to be able to produce PERFORMANCE reports for GLS SMT, So that I can respond to requests for a variety of PERFORMANCE REPORT more easily and timely.

[SCM-52] As a Manager/Admin I want to be able to obtain statistics for different activity types so that I do not have to manually go through workbooks to produce the required report. (e.g. The Corporate complaint team, would need the following report: Number of complaints, Themes/Trends; Nature of complaints; Region; Directorate and Complaints

Case Manager provides real-time management information dashboards and a full report generation tool. Reports can be built as templates for re-use, with users specifying the values for parameters such as date ranges, case types etc, when they generate the report. Report templates use industry standard query and template languages and so can be created and altered by authorised and trained users. Case Manager also provides a wizard based reporting tool that allows users to create their own reports using simple and quick to use click through forms.

As described above in response to requirement SCM-54 Case Manager includes both real time management information dashboards and a full report generation tool. Case Manager also allows reports to be scheduled for automatic execution and export to third party reporting systems for further analysis or integration into wider corporate reporting platforms.

Case Manager allows a wide range of report types to be generated including performance reports for specific teams or groups of users.

Case Manager's report generation tools allow report templates to be defined that produce the statistics required. These reports can then be run by authorised users on a regular basis to retrieve the statistics for that period. These reports can include numbers of cases, time spent, numbers of actions, status of cases and many more. Reports can also be based on categorisation and other properties of the case records to ensure that only relevant cases are included in each report.

IIZUKA Response to LCMS Requirements ITT

<p>Status) (MUST)</p> <p>[SCM-53] As a User, Given that a case has being flagged as high, medium or low risks I want to have the ability to generate reports based on the risk rating of cases so that I know the number of High, Medium or Low Risks cases that I worked on in a given period e.g. weekly, monthly or yearly (i.e. A matter can be high risk due to commercial or political sensitivities for example, but that doesn't mean that the case is always the highest priority in terms of work load).</p>	<p>Once cases are flagged with a risk then they can be presented to users through real-time dashboards or though management information reports. Reports can also be generated that only include statistics from cases depending on their risk,</p>
<p>[SCM-25] As a GLS team lead I need to view other team members case work and identify trends or gaps to support a better way of working so that</p> <ul style="list-style-type: none"> a). I can identify and respond to coaching requirements of team members, b). I can ascertain teams present capacity demands, c). I can provide internal quality assurance for the team 	<p>Case Manager allows authorised users, including team leaders, to access cases within and across teams. From within a case authorised users can access the case history, notes and other information recorded there. Case Manager also supports structured case reviews and quality assessments where the review is recorded within the case, but secured from normal user access, but giving the owner of the case the opportunity to respond to feedback and take corrective action.</p> <p>Capacity management is achieved through dashboards and management information reports that show the current and past allocation of work across individuals, teams and organisations.</p>
<p>Manage cases- Search, Archive & Retrieve cases</p> <p>[SCM-19] As a Legal Services team member I need the ability to record advise given to Clients i.e. Inspector regarding a Provider so that at any point in the future, there is reliable audit trail of all information documented about the case in line with CQC legal responsibility (GRAM- QUALITY REVIEW ASSURANCE MANAGEMENT).</p>	<p>Within a case, Case Manager allows structured records to be captured, including records of contact with clients and third parties. Actions can be configured to be of different types, with different fields and purposes. This allows a detailed record of contact and advice to be constructed. Each entry is recorded with the date and time at which it occurred and the user who recorded it. The historic actions are then clearly visible in chronological order within the case action history of the case. The types of actions and contact that can be recorded can be configured by authorised administrators within the system</p>

IIZUKA Response to LCMS Requirements ITT

	<p>administration area. As part of the implementation of the system, IIZUKA will analyse the specific requirements in this area and set up an initial configuration that meet's the CQC business need.</p> <p>Case Manager includes a fully featured search tool. Users are able to search for cases quickly by reference number or by details of the case or its contents. Users can also search for individual actions within cases, by any of their properties. In addition to manual search functions, Case Manager also automatically searches for the details of client's cases that have already been recorded. This reduces the likelihood of duplicating cases and allows related cases to be found and linked together.</p> <p>Cases are also linked to other records, such as records of external organisations, providers, lawyers etc. Where these links have been recorded, users can easily navigate lists of all cases linked to a specific record. For example a list of all cases involving a particular provider or with a particular lawyer.</p> <p>Users are able to search for cases by properties that apply to cases of all types or those that are unique to each type of case. The Complaints Team will therefore be able to search for complaint cases depending on the type of complaint. A dashboard can also be provided that identifies complaint cases that have yet to be reviewed, according to their type. During the requirements analysis phase IIZUKA will review this requirement with the Complaints Team and will advise on the best approach to using the system to meet this need.</p> <p>Cases in Case Manager have a status that identifies their position in the workflow of the case. When the case reaches a closing status it automatically disappears from dashboards and other active case lists, but is available to users through searching and linking from other cases.</p> <p>Case Manager also supports rule based anonymisation or deletion of cases, so that data protection legislation</p>
<p>[SCM-70] As a User, I want to have the ability to search for cases e.g. previous cases, previous advice or conflict, so that I am able to cross reference my work to avoid duplicating work in order to manage my time efficiently (Note: search case by legislation, lawyer, court, tribunal, sector, provider) (MUST)</p>	<p>Cases are also linked to other records, such as records of external organisations, providers, lawyers etc. Where these links have been recorded, users can easily navigate lists of all cases linked to a specific record. For example a list of all cases involving a particular provider or with a particular lawyer.</p>
<p>[SCM-71] As a Member of the Complaints Team, I want to have the ability to search for complaints by type, so that I can manage time spent on reviewing complaints efficiently (MUST)</p>	<p>Users are able to search for cases by properties that apply to cases of all types or those that are unique to each type of case. The Complaints Team will therefore be able to search for complaint cases depending on the type of complaint. A dashboard can also be provided that identifies complaint cases that have yet to be reviewed, according to their type. During the requirements analysis phase IIZUKA will review this requirement with the Complaints Team and will advise on the best approach to using the system to meet this need.</p>
<p>[SCM-68] As a User, I want to have the ability to archive cases, so that I can comply with legislation (MUST)</p>	<p>Cases in Case Manager have a status that identifies their position in the workflow of the case. When the case reaches a closing status it automatically disappears from dashboards and other active case lists, but is available to users through searching and linking from other cases.</p> <p>Case Manager also supports rule based anonymisation or deletion of cases, so that data protection legislation</p>

IIZUKA Response to LCMS Requirements ITT

	commitments are met. Typical configuration of this is to automatically delete or anonymise cases a set amount of time after their closure, unless they are specifically marked for retention or meet other specific criteria.
[SCM-69] As a User, I want to have the ability to retrieve archived case file so that I can look at cases related to cases that I am currently dealing with (MUST)	Closed cases are retained in the system and area easily accessible by users through searching or linking from other cases. Closed cases can also be re-opened if appropriate, depending on the configured case workflows.
[SCM-21] As a Legal Adviser, I need an appropriate retention policy to be applied to the case when it is confirmed as complete so that we are compliant with our records management policy, and CQC can adhere to the Public Records Act 1958 and Data protection Act 1998	Case Manager includes functions for automatically deleting or anonymising cases a set time after their closure. The rules for this are configurable by authorised administrators so as to meet the specific needs of the CQC in this area.
[SCM-72] As a User, I want to have the ability to retrieve files relating to the case I am working on so that I can continue working on it (MUST)	Once a user accesses a case, they can then retrieve any attached files or linked records, subject to their access level and the security permissions associated with the case and linked records.
[SCM-73] As a User, I want to have the ability to retrieve information regarding cases/advice so that I can respond to freedom of information request (MUST)	Case Manager allows the details of individual cases to be accessed when responding to FOI requests. The inbuilt reporting tool can also be used to identify cases and statistics in bulk in relation to FOI requests. Case Manager's configurable list of case types and workflows also means that it can be used by the CQC for managing FOI requests themselves; ensuring that statutory obligations are met efficiently.
Time Recording Cost & Fees	
[SCM-33] As a member of the legal team, I need to be able to record the time spent completing particular areas of legal work in order to submit a cost	Case Manager has a Time Recording module that allows users to record time against cases, against individual actions within cases or generally, where time is spent not working on specific

IIZUKA Response to LCMS Requirements ITT

<p>application to the court so that CQC can successfully recover cost incurred in providing legal services</p>	<p>cases. Time can be recorded quickly and easily as users complete actions. Time spent can also be categorised by users, to provide a clearer indication of what activity they were reporting on. A dashboard also provides users with a view of the total amount of time they have recorded for each day, so that they can ensure their time is accounted for. Time that has been recorded can be output in management information reports the include details of the time spent, by whom, of what types, and in relation to which cases, types of case or type of activity.</p>
<p>[SCM-56] As a System, I want to have the ability to record the time spent by a case worker on a case so that the accurate time spent on the case is recorded for costing purposes (MUST)</p>	<p>Case Manager retains the time recording records of all users and makes it available through management information reports. Time can be categorised in reports based on the types of time recorded, the types of the cases or actions to which it relates, the groups of users who have spent the time and many more. This allows detailed costing reports to be produced, with time correctly identified based on costing and reporting criteria.</p>
<p>[SCM-34] As a member of the legal team, I need to be able to record the time spent by external legal advisers in completing particular areas of legal work in order to verify the accuracy of fees application submitted to CQC so that CQC does not incur excessive fees</p>	<p>As an Internet hosted, multi-agency platform Case Manager allows external agencies to record actions completed and time spent securely. Where this is not desirable or not possible because of practical or business reasons, users can record time on behalf of third parties. Time recorded is then available in management information reports, allowing the CQC to determine the amounts of time spent and the impact on associated fees.</p>
<p>[SCM-32] As a legal Manager, I need to be able to assess the time spent on particular areas of work for succession planning so that I can allocate work more efficiently and for performance management</p>	<p>Case Manager's reporting tools allow the reporting of time spent, with breakdowns or filtering based on the type of time recorded, by whom and in relation to which types of cases and actions. These reports can also determine broad amounts of time spent on cases meeting certain criteria, such as subject area, geographical area, involved parties and others. This allows for both detailed planning and wider assessment of trends and</p>

IIZUKA Response to LCMS Requirements ITT

<p>[SCM-49] As a User (all users), I need to be able to ensure cases/tasks are dealt with in specified time as per business protocol so that I know that I meet all deadline (MUST)</p>	<p>general resources.</p> <p>Cases are managed in Case Manager through workflow, which ensures that key dates are recorded and monitored. Automatic prioritisation and alerts keep users informed as deadlines near. Personalised dashboards provide users with lists of actions that they are responsible for, or their team is responsible for, prioritised according to due dates and deadlines.</p> <p>When actions are completed Case Manager automatically records whether they were completed before or after the deadline, ensuring that historic records and management information reports accurately reflect the timelines of cases.</p>
<p>[SCM-57] As a User, I want to have the ability to record time spent on a case against given activities so that I know the total time spent on the case (For Example: If a case belongs to a given category or contract type, the user should be able to choose activity carried on the case from an activity list to show what task(s) they performed for the time spent) (MUST)</p>	<p>Case Manager's time recording module allows time to be recorded against cases or actions and categorised by type. Time that has been recorded can then be counted in total for teams, individuals, specific cases or based on criteria such as the type of time recorded or the attributes of the cases or actions against which it was recorded.</p> <p>This allows the system to generate clear outputs of what time was spent, by whom and doing what.</p>
<p>Digital Division of Labour</p> <p>[SCM-42] As a Legal Advisor (Manager) I need to assign sections of a case to different members of the Legal team (i.e. Paralegal, internal and external Legal Advisors), so that the relevant roles complete the appropriate sections and that we can work collaboratively and complete the case in good time</p>	<p>Case Manager allows cases to be assigned, but also specific actions within cases. Cases can also have multiple people assigned with different responsibilities on the case. Each users' actions are then tracked, both within the case itself and within personal and management dashboards. Alerts and work queues provide means by which cases are actively monitored across teams and disciplines, ensuring timely responses and efficient productivity.</p>
<p>[SCM-43] As a User I want to be able to carry out conflict of interest search so that duplication can be avoided as well as avoid a joined up response across the sector (MUST)</p>	<p>Users are able to search within Case Manager for cases depending on who was involved in them, and so quickly identify cases that might represent a conflict of interest. It also allows cases to be linked to records of people or organisations, so that all cases involving them can easily be</p>

Quality control feedback		identified.
<p>[SCM-22] As a legal member invited to an NQAG panel I need the report to have been circulated at least 5 working days (or appropriate time) prior to the NQAG so that I have sufficient time to review the report and be in a position to provide relevant legal advice, backed up by relevant evidence or previous precedence</p>		<p>Case Manager allows actions and reports to be scheduled in advance, according to workflows and configured deadlines.</p>
	<p>[SCM-23] As a member of GLS involved in the quality control of a case document I need to provide feedback to the author on a single source of the document so that</p> <ul style="list-style-type: none"> a). good version control practices are adhered to b). an accurate audit trail is maintained in order see and refer to the historical development of a document <p>Please describe how you are able to record the time spent completing particular areas of legal work in order to submit a cost application to the court?</p>	<p>Case Manager allows structured workflows to be configured that include quality control stages in the production of case responses. Quality control assessments can be structured with fields that guide users with prompts on what should be checked and assessed.</p> <p>Case Manager automatically logs all case updates and document changes in the audit log. This can be viewed by authorised users and can be viewed from within a case.</p> <p>Case Manager includes a time recording module that allows users to log amounts of time spent as they complete activities or work on cases. Users can easily enter time using a quick notation format, such as 1h6m, so time recording becomes swift and natural. Time records are automatically linked to the records of the case or actions that the user was working on. This allows reports to easily categorise time and produce total costs on a per case or category basis for submission to courts. Tools are also provided that enable users to see how much time they have logged in total, so as to make sure that their time is accounted for.</p> <p>Further functions allow users to record time spent on different categories of non-casework activities, and so give a fuller account of their time</p>

Annex D - Technical Merit for Non Functional Requirements – Generic SaaS

Non Functional Requirements – Generic Software as a Service Requirement		Compliance	Response
		Availability requirements & support	
System availability – Any system is required to meet service availability levels of 99.5% Monday to Friday 5 days a week with the exception of bank holidays. with system maintenance outside working hours	Full		Case Manager will be provided as a hosted managed service with contractual availability of 99.5% Monday to Friday 9am to 5pm. Most system maintenance can be applied without impacting the system, but where there is impact then planned maintenance will be scheduled outside of working hours wherever possible
Required server environments – The following server environments are required Live, Test, Development, User Acceptance Testing, Pre-production and Training, if appropriate to the nature of the service.	Full		The solution will be provided with Live, Pre-production, training and test environments. User acceptance testing will be conducted on the test environment and development will be conducted on separate environments at IIZUKA's offices. Further temporary environments can be created for special projects if required.
Disaster recovery – System will be supported in the event of a disaster and any recovery plans will be tailored to CQC needs and be compliant with business continuity standards.	Full		The system is provisioned to include Disaster Recovery support with detailed plans and periodic Disaster Recovery transfer tests. The plans will be coordinated with the CQC.

IIZUKA Response to LCMS Requirements ITT

Recovery Time		
Recovery time & point objective - The recovery mechanisms must support minimal recovery time with optimal recovery points.	Full	IIZUKA operates the system with a Recovery Time Objective of 4 hours and a Recovery Point Objective of 2 hours.
Backup schedules - Back-ups are to be carried out completely according to documented data back-up requirements. Appropriate personnel are to verify the usability of backed-up data and retain verification evidence.	Full	Backups are provided as part of the managed service and operate through regular log shipping to a secondary site in accordance with IIZUKA's accredited ISO 27001 procedures. Logs are shipped in 16mb batches, which on a typical day results in logs being transferred every few minutes. Tests of backups are conducted regularly and the results retained.
Performance & scalability		
Storage - The system must handle an increase in storage requirements without major system changes or data migration activities.	Full	The system is provisioned with storage capacity appropriate to estimated usage volumes and is backed by a Storage Area Network (SAN), but further space can be provisioned through expansion of the allocated SAN segment.
System scalability - System shall be scalable both in terms of users and storage, with that easy to change both in terms of cost and minimal disruption.	Full	The system is hosted as a managed service and is built on a scalable architecture running in a virtual server environment that includes load balancing across multiple servers. Scalability is easily achieved through the addition of further resources or additional virtual servers
Network performance and load - The system must minimise the load on CQC's network and provide mechanisms for reporting on and controlling that load.	Full	As an externally hosted managed service the system will have minimal impact on the CQC network. The majority of traffic will be HTTPS user traffic over the connection between CQC and the hosted solution. As a web-based solution Case Manager only needs to transfer HTML data and page resources to users' devices. These are kept as small as possible, with further strategies for compression and caching applied to further limit data transfer sizes. Integration from Case Manager to CQC systems will generate further network traffic

IIZUKA Response to LCMS Requirements ITT

<p>System performance - Describe the typical response time that can be expected from an end user perspective when accessing the application, carrying out a typical task.</p>	<p>N/A</p>	<p>but again this will be limited as the current scope only includes integration for the purposes of Active Directory authentication and MS Exchange integration. If required, the volume of data transferred between the CQC network and Case Manager solution can be monitored and reported, but given the expected user volumes of the system IIZUKA would not expect this to be required</p> <p>As a web based solution all actions by users result in full or partial reloads of pages within their web browser. Most operations within the system are completed in under a second, with typical response times for standard screens being around a third of a second. More complex operations may take longer but will typically not take longer than 5 seconds. User dashboards and other configurable displays of information will respond in a time that depends on their complexity so IIZUKA will advise the CQC where custom requirements for these are likely to result in high system load.</p> <p>IIZUKA monitors the performance of the system and conducts performance tests to ensure that users continue to experience high levels of responsiveness. Strategies for ensuring high levels of performance include caching, compression and database indexing</p>	<p>Case Manager will be implemented so as to authenticate users against the CQC Active Directory using ADFS and SAML as mandated in the CQC Technical Architecture Principles, on the assumption that the CQC elements of this technology are available and accessible to the levels required for an externally hosted system.</p> <p>The solution is capable of integration with the stated data sources and supports a wide range of integration options. The preferred integration route is web services using XML or JSON payloads and is fully compliant with SOA architectures such as Mulesoft. Please note that this capability is provided as standard, but specific integrations will need further development and configuration depending on the particular integration objectives and requirements. The only integrations included in the current scope of this response are authentication with the CQC Active Directory and calendar/email integration with MS Exchange</p>
<p>Integration - System must support authentication using CQC's existing active directory as part of its existing infrastructure managed service (Open Service) using ADFS.</p>	<p>Full</p>	<p>Full</p>	<p>Full</p>
<p>Interface requirements - Where relevant to its function, the system shall be capable of interfacing with CQC internal and external data sources, such as Siebel CRM, OBIEE, Oracle 11g, MySQL, PostgreSQL and SQLServer 2008 and above, making use of CQC's Mulesoft</p>			

IIZUKA Response to LCMS Requirements ITT

Anypoint platform for transactional integration. As stated in the Architecture Principles, a service oriented approach should be used, where practical and possible.		
Use of mobile devices - System shall support the use of a range of mobile devices, meeting CESG requirements.	Full	Case Manager is fully supported as a web based system accessible from the web browser on most modern mobile devices and is secured in accordance with the system security principles and accreditation. A mobile application for Android is also available as an additional option that supports off-line synchronisation and additional features such as photo upload and signature capture. The price for this option is available in request.
Monitoring		
Application monitoring - The application must be monitored by the provider, with suitable alerting tools in place to notify of current or imminent service breaches and security issues.	Full	The Case Manager solution is provided as a hosted managed service that includes monitoring at the infrastructure and application levels. Alerts are notified in real-time to the IIZUKA service desk. Where availability or security issues are identified the IIZUKA service desk will then notify the CQC through agreed channels, in accordance with contractual Service Level Agreements
Reporting		
Availability reporting - Provide examples of daily, weekly and monthly application availability reporting.	Full	Availability reporting is included in the monthly security report, an anonymised example of which is attached as 'Example Monthly Security Report'. Within each month, any availability affecting incidents are reported directly to the customer as they occur through agreed service desk channels.
Capacity reporting - provide examples of monthly reporting on current versus projected capacity, both in terms of storage and licenses.	Full	Licenses are not included in capacity reporting by IIZUKA as user licences are recorded in the system themselves and can be reported on by authorised users on demand. Total available storage capacity and current usage are listed in the monthly security report.
Service Management reporting - provide examples of daily, weekly and monthly	Full	IIZUKA provides a monthly service desk report, an example of which is attached as 'Example Monthly Service Desk Report'. Within each month significant issues (i.e. severity 1) are reported directly to the service desk manager through agreed

IIZUKA Response to LCMS Requirements ITT

reporting on the overall performance on the service, including performance, requests and incidents relating to the service.	channels.	
Change management and release		
<p>Change management</p> <p>Demonstrate your ability to perform changes to the application in a controlled and structured manner, including adherence to any methodologies.</p>	Full	<p>Case Manager is a highly configurable system that can be managed by authorised business users. IIZUKA will provide guidance and support to a project team nominated by the CQC. This will introduce them to the configuration of the system and gradually transfer ownership of that management to the CQC. Changes made in this way can be applied directly to the system by authorised users without impacting the availability of the service. Changes are typically developed and tested on the test environment, before being put through final checking on the pre-production environment and then deployed live. Such changes are considered 'routine changes' by IIZUKA and would therefore not go through formal individual change control features.</p> <p>Where such project staff are not available or where bigger changes are required that cannot be met entirely through in-system configuration, IIZUKA will follow its ISO 27001 and ISO 9001 accredited change management processes that are fully compliant with ITIL best practice. Proposed changes are documented in formal change requests, which are then subject to authorisation by the Change Advisory Board (CAB) before being finalised and deployed after testing and staging through appropriate environments.</p> <p>IIZUKA typically sits on the CAB with key members of the customer and other partner service providers. This allows IIZUKA's expertise to be used in understanding the impact on the system of any proposed change.</p> <p>If configuration by the CQC itself is not desired or practical then configuration duties can be delegated back to the IIZUKA service desk subject to commercial agreement.</p>
<p>Release Management - System to be subject to formal processes for release management, in</p>	Full	<p>Releases are performed through IIZUKA's ISO 27001 and 9001 accredited release management procedures. All software releases are developed at IIZUKA's development offices and put through rigorous development procedures with</p>

IIZUKA Response to LCMS Requirements ITT

<p>association with customer with regard to testing.</p>		<p>automated and manual testing. Once authorised, releases are made available to customers in a test environment for user acceptance testing. IIZUKA provides test support during this period and any identified defects can be addressed or noted for future correction. Once the acceptance is achieved releases are staged through the pre-production environment before deployment to the live system. Deployment of releases to the live environment can only be performed under authorisation of the CAB after submission of a Deployment Request change control document by IIZUKA. Most releases can be deployed to the live system without impacting availability of the live system, but where this is not possible the deployment will be performed at an agreed scheduled time.</p>
<p>Segregation of environments - Responsibilities related to program coding, application testing and approval, program transfer between environments are segregated</p>	<p>Full</p>	<p>Environments are logically separated from each other at the infrastructure level with no ability for inter-environment communication between instances of the system. All program coding is conducted at a separate physical location and within IIZUKA's development network, which is separate from the hosting infrastructure. A separate OPS network is used by IIZUKA when access to the live or other hosted environments is required for deployment or support. Each environment has a dedicated database within the infrastructure, with each using separate credentials and keys that are not held within the other instances. Service desk and system administrators have distinct logins for each separate environment to prevent the risk of accidental usage of the incorrect environment.</p>
<p>Language support - The application must support UK English.</p>	<p>Full</p>	<p>The application is built to support UK English</p>
<p>Desktop support - All system configuration settings are remotely accessible to the system administrator through application screens or setup programs (i.e. no hard coded system variables exist and include system, user, roles, company and other configuration screens).</p>	<p>Full</p>	<p>The system includes a fully featured administration area where authorised users can configure fields, contact details, access levels, roles, case types, action types, workflow, message templates, report templates, dashboard widgets, document templates and many more features of the application. IIZUKA will work with a nominated project team during the implementation of the project to transfer knowledge and ownership of this configuration to the CQC. IIZUKA service desk staff are also able to provide ongoing assistance and can take on this configuration role, by commercial agreement, in the event that CQC do not wish to take on the configuration themselves.</p>

<p>User experience – The solution must provide an intuitive user interface that enables the user to complete a task whilst minimising the need to navigate the system</p>	<p>Full</p>	<p>Case Manager has an intuitive, web based user interface that presents information through a consistent and logical information architecture. Users are able to use normal web browsing conventions and can bookmark pages, work in more than one browser window simultaneously and use the 'back button' except immediately following a form submission. Please refer to the example screen shots included in the functional requirements response</p> <p>Case Manager also supports configurable views of information, allowing regularly accessed information to be combined into easy to access displays.</p>
<p>Software as service - Customer Desktop devices are restricted in terms of the ability to download components from external sources. The system shall operate with the minimal need for software components to be applied to PC or desktop devices. The CQC standard desktop is Windows 7 32 bit with 3.5 Gb of RAM with Internet Explorer 10 and Microsoft Office 2010. In the future a 64 bit client may be used and any client software should be able to take advantage of that and increased memory availability. The supplier must provide comprehensive systems administration, installation guides and processes, as appropriate to the nature of the service.</p>	<p>Full</p>	<p>Case Manager is accessible through standard web browsers and is currently supported on the latest version of all major browsers. Internet Explorer 10 is no longer supported by Microsoft and so we cannot formally support it. Customers are recommended to upgrade to IE 11 or use an alternative browser. Internet Explorer 10 is generally compatible with Case Manager and can be used at the customer's own discretion, but formal support is not provided.</p> <p>Should the CQC upgrade to a 64 bit client then Case Manager is already fully compatible with this.</p> <p>As a hosted managed service no systems administration or installation guides are required.</p> <p>Please refer to the attached document 'Typical Deployment Architecture' which shows an outline of a typical Case Manager Deployment architecture suitable for this level of solution. Please note that this is for illustration purposes only and the final deployment architecture will be devised as part of the design and implementation of the solution.</p>

IIZUKA Response to LCMS Requirements ITT

A complete, typical deployment architecture must be described.		Compliance	
Open service IT standards - The application must comply with the CQC Architecture Principles.	Full	Please refer to the separate document 'Technical Architecture Principles Response'	
Legal compliance - Compliance to all U.K. legal requirements including the Data Protection Act (1998), the Freedom of Information Act (2001) & Privacy laws.	Full	The solution is hosted in line with the stated legal requirements. IIZUKA's accredited ISO 27001 procedures ensure that relevant changes in legislation are identified and compliance maintained	
Government Technology Strategies – The system or service must comply with the U.K. Government Digital strategy	Full	The solution is fully in-line with the government data strategy and is used by a wide range of government customers	
Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.	Full	Case Manager includes a bulk deletion or anonymization function that automatically selects records for purging depending on configurable retention rules. Purging uses a set of rules to ensure that interlinked records are only deleted under the correct circumstances and so as to maintain data integrity.	
Escrow			
Source code availability - In the event of buyout or liquidation of the vendor the base source code of the software must be made available to CQC.	Full	The system source code will be deposited with a third party ESCROW agent as a 'basic' deposit and will be released to CQC in the event of buyout or liquidation.	
Support			
Service desk & service manager - Supplier shall provide a service desk with the	Full	IIZUKA provides a service desk for the resolution of incidents and customer support requests. The service desk is available from 9am to 5pm on Mondays to Fridays, excluding UK public holidays. Support is available via email and telephone.	

IIZUKA Response to LCMS Requirements ITT

ability to log and resolve incidents and requests. The supplier shall provide a named contact for escalation of issues and regular interface between the supplier and the customer. The supplier shall detail the channels available and typical response times for both fault resolution and functional query support.

Severity 1 incidents must be reported by telephone, but can be supplemented with an email. IIZUKA will nominate a service manager as the escalation point for the CQC and they will provide the monthly service desk report and liaise with the CQC as required.

Response times for fault resolution are as per IIZUKA's standard terms and conditions below:

Severity level	Definition	Response time	Resolution target (SSHs)	Examples
1	Failure of business critical function	30 minutes	4	Main business use interruption (e.g. unable to process cases or to run report at month end). Apparent loss of business critical data.
2	Defect in high usage function	30 minutes	16	Functional error preventing use of specific screen within a case (e.g. unable to record notes).
3	Defect in low usage function	30 minutes	40	Search returning incorrect results. Failure to send reminder emails.
4	Non-functional defect	30 minutes	By agreement	Inconsistent sorting, unintended process outcome. Typographical or layout error.

The response times for customer support queries is 30 minutes.

Service Credits:

If your service is unavailable as a result of a failed hardware component, and IIZUKA fails to meet the guarantee stated in the SLA, you are entitled to a credit in the amount of five per cent (5%) of your monthly recurring fee per half hour of down-

IIZUKA Response to LCMS Requirements ITT

		time (after the initial four (4) hours of SLA downtime) for the affected service, up to one hundred per cent (100%) of the monthly recurring fee for the service for any calendar month.
Accessibility		
Accessibility – The system shall enable accessibility via assistive technology for those who cannot use a standard mouse and/or keyboard e.g. WA3, Dragon Speak and Windows 7 Voice Recognition software. It shall also enable access for those with additional visual or hearing needs. The supplier shall state how these needs are met by the software.	Full	Case Manager is fully compliant with WAI accessibility guidelines and is widely used by users of assistive technologies. All screens are written in standards compliant HTML and have been tested with a range of screen readers and dictation software. Users are able to adjust text sizes and zoom levels via their web browsers. As part of the implementation process IIZUKA will test the system with the particular software in use at the CQC and attempt to rectify any defects so as to improve the experience for users with accessibility needs. Voice recognition is supported through standard web browser features that allow dictation of text into highlighted fields.
Integrate with Outlook / MS Exchange: Describe the security mechanisms and protocols to be used for integration with MS Exchange for the creation of calendar events and sending of emails on behalf of users.	Full	Case Manager supports integration with MS Exchange through the Exchange Web Services API. Please refer to our more detailed response in the Technical Architecture Principles Response document. Please note that integration with Exchange is not required for Case Manager to send emails as the service includes a managed SMTP relay.
Describe the identification and authentication procedures and protocols to be used and any supported federation mechanisms available.	N/A	Case Manager supports a wide range of authentication systems including integrated user login, Kerberos, HTTP basic authentication, LDAP/Active Directory, SAML and specialist two factor authentication systems. The CQC Technical Architecture Principles mandate the use of Single Sign On, against the CQC active directory via Active Directory Federation and support for SAML2 tokens. This is compatible with Case Manager so IIZUKA proposes to use

		this approach for the solution.
--	--	---------------------------------

Appendix E - Technical Merit for Non Functional Requirements - Information Security

Non Functional Requirements – Generic Software as a Service		
Requirement	Compliance	Response
Session security		
Login – All user identifiers must be linked to roles which have explicit and granular assignments to access levels that enforce a restriction on the ability of the end user to create, read, update and delete information.	Full	Case Manager includes a comprehensive Role Based Access Control (RBAC) model that ensures users are only able to access data and functions to which they are granted privileges. Super users are able to define the different levels of access and grant these to users through the allocation of roles. Roles support separate control over permission to read, create, update or delete information.
Password requirements – Passwords must be configurable and enable enforcement to have a minimum length of 8 characters with a mixture of lower and upper case characters and symbols, as required by CQC policies which may vary between devices. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.	Full	Case Manager includes a secure password management system that can be configured by authorised administrators. This allows minimum password strength requirements to be defined, meeting the stated rules. Automatic password expiry can also be enabled with a configurable period, but it should be noted that this is against current CESG best practice guidelines.
Password requirements for administrator accounts – Passwords for administrator accounts must be configurable and enable enforcement to have a minimum length of 10 characters with a mixture of lower and	Partial	Case Manager does not currently support differing levels of password strength for different types of user. If this strength is required IIZUKA recommends that it is specified for all users.

IIZUKA Response to LCMS Requirements ITT

upper case characters and symbols. Password expiry must be configurable and able to be set to 90 days and passwords must not be able to be recycled.			
Inactivity timeout – Where the solution maintains a user session, it must be able to configured to timeout as needed for the particular use case.	Full		Case Manager automatically times users out after a period of inactivity. The period is configurable at the server and can be altered through a request to the IIZUKA service desk.
Identity			
Client applications – The solution will identify all client applications before allowing them to use its capabilities.	N/A		The system is accessed through a web browser and does not support the use of client applications. Integrated systems are authenticated at the web service layer.
End users – The solution will identify all of its human users before allowing them to use its capabilities.	Full		Users are forced to login before they can access any feature of the application.
Physical access – All personnel will be required to present relevant identification before they are allowed access to secure locations such as CQC offices or data centres.	Full		All IIZUKA staff are SC cleared and will present identification on attendance.
Single sign on – The solution will not require an individual user to identify themselves multiple times during a session (single sign on).	Full		Case Manager supports single sign on within the application via a configured trust relationship with the CQC Active Directory as required by the Technical Architecture Principles
Inactivity – The solution must provide a mechanism for suspending user accounts when they have not been used for a predefined period.	Full		Case Manager does not automatically expire unused user accounts, but a report is provided of users that have not accessed the system in the specified period and allows them to be deactivated by authorised users.
Employee status – The supplier must prevent access to customer data and	Full		All IIZUKA staff are vetted to SC level and must comply with IIZUKA's ISO27001 accredited information security principles as a condition of their

IIZUKA Response to LCMS Requirements ITT

systems by employees who are leaving its employment and disclose their policy and procedures regarding this.		employment. Copies of IIZUKA's ISO 27001 policies and procedures can be made available by special arrangement.
Authentication		
Access to capabilities – The solution will authenticate all users before allowing them to use its capabilities.	Full	Users are forced to login before they can access any feature of the application.
Access to user details – The solution will authenticate of all users before allowing them to update their user information.	Full	Users are forced to login before they can access any feature of the application
Access by client applications – The solution will authenticate all client applications before allowing them to use its capabilities.	Full	The system is accessed through a web browser and does not support the use of client applications. Integrated systems are authenticated at the web service layer.
Authorisation		
Own personal information – The solution will allow each user to access to all of their own personal information, where applicable.	Full	Users have access to their own personal information through a link on their dashboard after logging in to the system.
Access to user details – The solution will authenticate of all users before allowing them to update their user information.	Full	Users are forced to login before they can access any feature of the application
Access by client applications – The solution will authenticate all client applications before allowing them to use its capabilities.	N/A	The system is accessed through a web browser and does not support the use of client applications. Integrated systems are authenticated at the web service layer.
Authorisation		
Own personal information – The solution will allow each user to access to	Full	Users have access to their own personal information through a link on their dashboard after logging in to the system.

IIZUKA Response to LCMS Requirements ITT

all of their own personal information, where applicable.			
Others personal information – The solution will only allow users access to the personal information of other users, where a business case for that exists.	Full		Access to information within the system is configured through a configurable Role Based Access Control (RBAC) model.
Access restrictions – The solution will be capable of restricting access to specified areas or databases.	Full		Access to information and functions within the system is configured through a configurable Role Based Access Control (RBAC) model.
Password repository – The solution will not allow access to the user password or hash database / file.	Full		Passwords are stored in encrypted format in the system database and cannot be accessed in the unencrypted form.
Incorrect credentials – The solution will create increasing time periods between the entry of incorrect credentials in order to prevent brute force passwords or denial of service attacks.	Full		User accounts are automatically locked for a configurable amount of time after a configurable number of incorrect login attempts has been made. Case Manager does not currently support automatically increasing time periods, but this could be added as a custom extension if required, at further cost.
Immunity (AV) and			
Threat identification – The solution will protect itself from infection by scanning all entered or downloaded data and software for known computer viruses, worms, Trojans and other similar harmful programs.	Full		All uploaded files are automatically virus checked before they are stored in the system. Files that fail the check are rejected.
Threat removal – The solution will be capable of disinfecting or quarantining any file found to contain harmful programs.	Full		Case Manager will not accept files that fail virus checking
Threat alerting – The solution will alert an administrator of any harmful	Full		Logs entries are created when files fail virus checking and these can be used as an alert trigger for administrators

IIZUKA Response to LCMS Requirements ITT

software found during scans.			
Threat currency - The solution will regularly (daily or weekly) update the anti-virus definition files.	Full		Anti-virus definition files are regularly updated as part of the managed service
Innovation - Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.	Full		IIZUKA uses best of breed virus checkers and regularly evaluates their use
Intrusion Detection and Protection			
Authentication failure - The solution will detect, prevent and record all access attempts which fail identification, authentication or authorisation requirements.	Full		All successful and unsuccessful login attempts are recorded and made visible to authorised administrators through a special administration area
Intrusion notification - The solution will be capable of reporting on all failed access. The application will notify the administrator(s) within 5 minutes of the IPS system triggering alerts.	Full		The solution includes a best of breed Intrusion Detection System that supports fully configurable alert levels and is analysed by a specialist team of network security specialists. Alerts are sent by email immediately upon trigger.
Innovation - Due to the increased level of innovation in threat creation, the means by which evolving threats will be addressed must be demonstrated.	Full		IIZUKA selects best of breed IDS solutions that have a continual upgrade programme and a dedicated net security monitoring team
Physical Access - Where connectivity is provided to end point devices network access controls must be in place to ensure that only authorised and secured endpoints are able to access network resources.	Full		Case Manager is provided as a hosted managed service that is accessible across the Internet. This can be restricted to trusted end points, subject to alternate requirements for remote access and home workin

IIZUKA Response to LCMS Requirements ITT

Audit			
Audited elements - The business elements that will be audited must be stated explicitly.	Full	Case Managers audit log covers all business elements configured in the system	
Audited fields – The data fields that will be audited must be stated explicitly.	Full	All data fields are audited	
Audit logs – The audit logs should be configurable to record activities appropriate to the system.	Full	All activities are audited, including views, creates and edits of all record types	
Enhanced privileges – A record of all activity by accounts with enhanced privileges must be retained for three months.	Full	All activities are audited and records kept for more than three months	
Audit status - The solution will collect, organise, summarise and regularly report the status of its security mechanisms.	Full	The audit is accessible by authorised users in the system administration area. IIZUKA will produce a regular security report summarising significant security events and statuses	
Security			
Data – The solution must be include security measures and controls suitable for holding data up to and including OFFICIAL SENSITIVE, where required.	Full	Case Manager is offered as a secure managed service that can hold data up to OFFICIAL SENSITIVE. Please note that further accreditation of the system that may be required by the CQC is at the CQC's cost. IIZUKA will fully cooperate in the activities required to achieve further accreditations but reserves the right to charge for additional accreditation activities	
Disposal – The solution must provide for the secure deletion of any information held on behalf of the customer as the result of the disposal of equipment or change or cessation of the service.	Full	All data storage media is securely disposed of in accordance with IIZUKA's accredited ISO 27001 procedures.	
Patching – CQC must be notified when patches or fixes are released for the solution	Full	Case Manager is supplied as a hosted managed service, so patches and updates are applied by IIZUKA as part of the managed service. Full release notes for new versions are provided that indicate what fixes are contained	

IIZUKA Response to LCMS Requirements ITT

<p>and provided a means to access and apply at short notice any urgent patches resulting from a security exposure. Patching support must be continued for old versions of the software and must be continued for a minimum of two years after the release of a major version that supersedes the prior version. This must be included as part of the support and maintenance costs.</p>		<p>within the update. Support for old versions is not applicable to a hosted managed service.</p>
<p>Credentials – The solution must not persist its own user credentials at the presentation or application layer and not persist any external credentials except through the use of tokens.</p>	Full	<p>All credentials used by the system are stored only in encrypted form and are deciphered using un-shared keys.</p>
<p>Authentication and access – The solution shall support 1user account per user. The service shall be demonstrably capable of segregating access to functions and data based on roles for specific users. This must include the ability to control access to create, read, update and delete functions acting on the data objects managed by the software.</p>	Full	<p>Case Manager includes a fully configurable RBAC model that governs access to data and functions with separate control over create, read, update and delete functions. The configuration of the RBAC is managed in the administration area. Reports are also provided that give a simplified overview of the current RBAC configuration</p>
<p>Identity & access management</p>		
<p>Formal approval of user changes – the solution must provide an audit trail of all user account and access management actions such as creating, amending and removing.</p>	Full	<p>All operations on user accounts and other configuration are audited, indicating the change that was made, the date and time and the user auctioning the change.</p>
<p>Account lock out - The number of failed login attempts before system lockout is 5 attempts or less and this value is able to be configured by an</p>	Full	<p>Accounts are automatically locked after a configurable number of failed attempts. Accounts are locked for a configurable amount of time. Configuration of these elements is done through a dedicated system administration area that is only available to privileged users</p>

IIZUKA Response to LCMS Requirements ITT administrator.

<p>Database access restrictions - For solutions that have a separate database, such as SqlServer or Oracle, access to the database must be able to be restricted to appropriate and authorised personnel only. For solutions that have a separate database, database accounts and their roles/groups are reviewed periodically for appropriateness. The solution must not use hard coded identifiers or passwords to connect to the database.</p>	Full	Direct access to the database is not possible for users from the application itself. Only authorised staff from IIZUKA and the hosting provider have access to the database. All accounts with database access are monitored and regularly reviewed. Database account details required by the application tier are stored in encrypted format and deciphered using and un-shared key
Integrity		
<p>Integrity - The solution will maintain the integrity of data and have appropriate controls and segregation of access to securely manage data throughout the data lifecycle.</p>	Full	Case Manager uses a relational database with inbuilt constraints to ensure that data integrity is maintained at all times. All interactions between the application tier and database are transactional and are rolled back in the case of an error occurring during the execution of a transaction
<p>Audit of use - The solution must demonstrate the ability to be configured to generate an accessible log of users' access to data for Create, Read, Update and Delete.</p>	Full	All data access is logged in the application audit log automatically. The log is visible to authorised users through the system administration area. The log viewer allows filters to be used to narrow the list of audit records to be displayed
Non-Repudiation		
<p>Non-repudiation - The solution will securely segregate and store all data (logs) relating to user actions on the system(s) including:</p> <ul style="list-style-type: none"> • Actions carried out i.e. read, write, change 	Full	All data access is logged in the application audit log, including read, create, update and delete operations. Audit logs include the identifier and summary of the record that was affected along with the date and time of the operation and the identity of the user

IIZUKA Response to LCMS Requirements ITT

<ul style="list-style-type: none"> • Date and time actions were carried out • The identity of the user by unique credentials 		<p>Compliance</p> <p>Legal compliance - Compliance to all U.K. legal requirements including the Data Protection Act (1998), the Freedom of Information Act (2001) & Privacy laws.</p>	Full	<p>The solution is hosted in line with the stated legal requirements. IIZUKA's accredited ISO 27001 procedures ensure that relevant changes in legislation are identified and compliance maintained</p>
<p>Data purging/archiving - There should be a mechanism for purging and archiving data in accordance with an agreed data retention policy.</p>	Full	<p>Case Manager includes a bulk deletion or anonymization function that automatically selects records for purging depending on configurable retention rules. Purging uses a set of rules to ensure that interlinked records are only deleted under the correct circumstances and so as to maintain data integrity.</p>		
<p>Escrow</p> <p>Source code availability - In the event of buyout or liquidation of the vendor the base source code of the solution must be made available to CQC.</p>	Full	<p>The system source code will be deposited with a third party ESCROW agent as a 'basic' deposit and will be released to CQC in the event of buyout or liquidation.</p>		
<p>Data centre</p> <p>Physical damage - The data centre will protect its hardware components from physical damage, destruction, theft or surreptitious replacement.</p>	Full	<p>Case Manager is hosted in ISO 27001 accredited data centres with strong physical access controls. Physical access to the data centres is by prior arrangement only and only under supervision of the hosts. A disaster recovery mechanism is used to ensure ongoing operation in the event of a catastrophic failure or physical damage.</p>		
<p>Hosting - The system must be hosted by an ISO27001 accredited organisation and must also be demonstrably capable of holding data up to and including OFFICIAL SENSITIVE. Patching must take place in line with the software</p>	Full	<p>Case Manager is hosted by an ISO 27001 accredited organisation and can hold data to OFFICIAL SENSITIVE. Patching of the application and its supporting infrastructure are part of the managed service. High priority patches are applied as required, with other patches applied on a regular basis.</p>		

IIZUKA Response to LCMS Requirements ITT

manufacturer's recommendations and be able to be applied at short notice in the event of a security exposure being identified. This must be included as part of the support and maintenance costs.			
Death and injury - The data centre will protect staff from death and injury.	Full	Access to the data centre is restricted, supervised and by prior arrangement only	
Physical application access - The application will be protected against unauthorised physical access.	Full	Access to the data centre is restricted, supervised and by prior arrangement only	
Maintenance			
System maintenance - System maintenance will not violate any of the security requirements as a result of upgrades or replacement of hardware, software or data.	Full	System maintenance is performed in accordance with the accredited ISO 27001 and procedures.	
Additional cloud services requirements			
Data ownership - All data remains the property of CQC and may not be used by the contractor except for processing as directed by CQC.	Full	IIZUKA is a registered data processor and all data remains the property of the CQC	
Documentation			
Required documentation - The implementation of each security requirement must be documented and approved by named individuals and distributed on an explicit and controlled circulation.	Full	The implementation of the system will be documented in a High Level Design that describes how security requirements are met. IIZUKA will facilitate a Security Working Group for the solution and this group will typically be the approvers of the security implementation	
Data purging/archiving - What is your data retention policy?	Full	Data within the solution is retained in line with a configurable retention policy. A typical policy is to retain data for 3 years after case closure unless specifically marked for retention, however this will be reviewed with the CQC	

IIZUKA Response to LCMS Requirements ITT
Appendix F - Technical Architecture Principals

Describe with specific reference the technical architecture principals how it is intended to deliver the solution that meets the architecture principals.

IIZUKA proposes to deliver a solution to the CQC that is based on its proven Case Manager platform. Case Manager is delivered as a cloud based managed service and is already built to the high standards required to meet the technical and security requirements of the CQC project. The table below describes how the proposed solution meets each of the technical architecture principles:

Principle	Compliance	Response
4.1 Staff can access systems wherever and whenever they need to	Full	<p>Case Manager is deployed as a secure cloud based solution that is accessible to authorised users via the Internet. This allows users to access the system from office based locations, home or anywhere that a sufficiently capable data connection is available. The system can also be accessed by users on mobile devices that have mobile data connections or on laptops tethered via mobile data connections.</p> <p>As a real-time system, supporting collaborative working, real-time alerts and other dynamic features, Case Manager's main functionality requires users to have an active connection. However the Case Manager Mobile application is also available for Android platforms that allows users to access and update cases and actions that have been assigned to them from their mobile device whilst it is offline. Data is then synchronised with the main system when a connection is available. Please note that this option has not been included in the proposed response as there are no stated requirements that described a need for offline remote working, but it is available as an optional extra if required.</p>
4.2 Applications are independent of technology platforms	Full	<p>Case Manager is a server based application that is accessed by users via their HTML compliant web browser. Case Manager supports the current versions of all major web browsers including Chrome, Internet Explorer, Edge, Firefox and Safari from both computers and mobile devices</p> <p>Case Manager itself is written using industry best practice approaches, in platform independent languages and using open source elements wherever possible. The</p>

IIZUKA Response to LCMS Requirements ITT

		<p>core application code is written in Java and is compliant with the JEE standard, so can be deployed to application server platforms running Unix, Linux or Windows operating systems. Data storage uses a standard SQL relational database with the standard option using PostgreSQL, but with MS SQL Server available as a further option.</p> <p>Integration and communication with other systems are achieved through best practice approaches using web services, typically with XML or JSON payloads</p>
4.3 A Service Orientated Architecture must be used	Full	<p>Case Manager user web services for integration and within the application. These are fully compliant with a Service Oriented Architecture and can be integrated with the CQC's existing Mulesoft SOA platform</p>
4.4 Bulk data exchanges use Extract Transform Load tools	Full	<p>Where possible IIZUKA recommends that web service based direct integration is used for communication of data with external systems, but where bulk data import or export are required Case Manager provides standard functions to support it. Case Manager provides both bulk import and export tools that allow data to be transferred in and out of the system using standard data formats such as XML and CSV files. This is managed using templates that can be configured to support different structures of data for import and export.</p> <p>Where these options aren't appropriate, Case Manager's data is held in a standard relational database so a wide range of ETL tools can also be used.</p>
4.5 Technical diversity is controlled	Full	<p>Case Manager is delivered as a service, so the internal technology is of limited relevance to the CQC, however some elements of the system are available to authorised administrators where greater control over configuration can be performed. The majority of these features do not require technical skill, however some elements allow users direct control over templates and scripting. In these cases a core set of languages are used that are well supported and publicly available, including XML, HTML, SQL, JPQL and Freemarker</p>
4.6 Interoperability standards must be used	Full	<p>Case Manager provides web service based integrations that use interoperable standards for data transmission. A wide range of options is available, but typically data is exchanged using XML, CSV or JSON payloads</p>

IIZUKA Response to LCMS Requirements ITT

4.7 Network quality must be maintained	Full	<p>As a cloud based managed service Case Manager does not directly impact the CQC network, however it is designed and managed so as to allow easy access from customer networks. Access is via standard HTTPS traffic, using HTML that is of minimal size and complexity, meaning that the load placed on the client's own network and bandwidth is minimal.</p> <p>The network within the Case Manager service is managed as part of the service and is continually monitored to ensure that capacity and reliability are appropriate.</p>
4.8 Software must be deployed on an infrastructure that will enable it to perform well	Full	<p>Case Manager is deployed as a managed service which included the infrastructure required to operate it. This infrastructure is continually monitored so as to ensure that it meets the required capacity and is performing well.</p>
4.9 IT systems are preferably open source	Partial	<p>As a managed service the source code of Case Manager is not directly relevant to the implementation of the solution for the CQC. Case Manager is a commercial product and is not fully open source, however it makes wide use of open source libraries and IIZUKA are active contributors to open source projects.</p>
4.10 Single Sign-On (SSO) must be supported	Full	<p>Case Manager supports integration with Microsoft Active Directory through standard authentication protocols, TODO explicit protocols in here.</p> <p>Through this, Case Manager supports single sign on for users using their Active Directory credentials. Users' permissions and levels of access within the Case Manager system are managed within Case Manager itself. with tools being provided to assist in the bulk management of user permissions</p>
4.11 Technology must be established and maintained	Full	<p>Case Manager is a highly configurable system and IIZUKA implements the system in partnership with the customer, so as to ensure that knowledge of the solution and its configuration is gained by the customer. This allows the customer to take on administrative control of the application to make business configuration changes so as to match changing requirements or new legislative or business needs.</p>
4.12 Applications are delivered using open	Full	<p>Case Manager is built using open standards wherever possible and IIZUKA has contributed to the development of standards. Where data is interchanged with</p>

IIZUKA Response to LCMS Requirements ITT

standards	Case Manager IIZUKA uses open standards as the formats of that data.
4.13 IT systems are scalable	<p>Case Manager is a scalable cloud based managed service that supports a vast range of customer volumes from single user systems to those with many thousands of users. The solution proposed has been sized to account for the level of performance appropriate to the current needs of the CQC, but this will be continually evaluated throughout the life of the project and options exist to quickly scale or reduce the solution so as to meet changing loads.</p> <p>IIZUKA also conducts regular performance tests of the solution so as to ensure new developments and features do not adversely affect the solution</p>
4.14 End-to-end security must be provided using multiple defensive strategies	<p>Case Manager is deployed as a cloud based managed service and is used to hold information to OFFICIAL SENSITIVE classification. Security is provided through numerous defensive strategies. The data centres, hosting provider and IIZUKA themselves are all ISO 27001 accredited, ensuring that they are built and managed in line with security best practice. IIZUKA holds Cyber Essentials certification and is in the progress of increasing this to Cyber Essentials Plus, which is expected to be within the time frame of this CQC implementation.</p> <p>Case Manager includes a comprehensive Role Based Access Control (RBAC) model that allows control over access to both data and functions.</p> <p>The solution includes a number of defensive technologies including monitored Intrusion Detection System and learning Web Application Firewall. All data transmission is encrypted and data at rest is encrypted at the storage level.</p> <p>The solution has been independently penetration tested and has been accredited by some of IIZUKA's government customers. IIZUKA assumes that if further accreditation is required by the CQC then this will be performed by the CQC at its cost, but IIZUKA will assist in the process; reserving the right to charge for additional work if required</p>
4.15 Integration with external IT systems is localised in dedicated IT	<p>Case Manager is compatible with the use of Mulesoft as an integration point for integrations with CQC systems that may be required. Please note that no integrations through Mulesoft are proposed in the current scope of this response as the only integrations defined in the requirements are with MS Exchange (please see</p>

Integrate with Outlook / MS Exchange: Describe the technical mechanisms and protocols to be used for integration with MS Exchange for the creation of calendar events and integration of email messages sent / received by users.

Case Manager supports integration with MS Exchange via Exchange Web Services. Case Manager's appointment booking elements will record user's appointments that have been booked through Case Manager into their Exchange calendar. Case Manager also displays the contents of the user's Exchange Calendar when booking appointments so that the user booking the appointment can see the availability of the person the appointment is being booked for.

Case Manager can integrate with Exchange in order to take copies of emails that are sent and received by users. This function however requires customisation and is not implemented as standard by IIZUKA, because experience shows that the results are of variable quality. The naturally unstructured form of emails means that determining the correct case to which the email should be related can often be problematic, especially where complex and interrelated cases exist. Case Manager customers also find that they use email less for communication between staff and with partner agencies as most communication occurs through the system. Furthermore emails sent in relation to cases are usually sent from within Case Manager and therefore do not require integration with Exchange. For these reasons Case Manager customers do not typically have Case Manager automatically capture emails. However, if this feature is required (please note that this is not explicitly stated in the LCMS Functional Requirements document) IIZUKA will assess the types and formats of email communication used by the CQC and determine the best ruleset to use to automate the collection and linking of emails to cases.

As an externally hosted managed service Case Manager will require authorised access and a secure route to the CQC Exchange server. IIZUKA assumes that CQC are able to enable access to Exchange Web Services from outside the CQC network and that a mailbox account can be allocated to the Case Manager system. This account will require privileges in Exchange granting read and write access to CQC users' mail boxes. IIZUKA will provide the scripts required to configure these privileges, but it will be the responsibility of CQC to run them and to make sure that they are applied to both existing and new users.

Please describe how you will deliver training including how many people will you offer to provide bespoke training and for how long? Describe what aftercare support will be provided?

Training

IIZUKA can offer a wide-range of training options to CQC but for the purposes of this project, IIZUKA will be offering classroom style train-the trainer approach with a blended, light-touch e-learning solution to augment training and support the users post training. This approach is the most effective and represents best value to our clients.

We can and have developed full managed, virtual learning environments for clients who have hundreds to thousands of users and this is something we can discuss with CQC as a potential option in the future.

A days training per user group is sufficient for Case Manager as the interface is intuitive and easy to navigate. Within Appendix A, CQC mentions 10 user groups who would all have some access to Case Manager based on their role. IIZUKA would work closely with CQC to identify what the appropriate training needs are per role and then design the training materials accordingly. In our experience of user groups of this size only one trainer for approximately 10 days will be needed. A duplicated training site that mirrors live will also be provided as an ongoing service.

After care support

Commercial and technical account managers are assigned for the duration of the project. These valuable team members will get to know and understand the project and the organisations aims in detail and provide help to ensure project success. Regular account review meetings will be held at CQC's convenience. These meetings will review the overall performance of the platform from an SLA, commercial and quality point of view.

IIZUKA has its own helpdesk that provides support to its clients. It's standard hours of support are 9:00 to 5:00. Variations to these times can be negotiated with up to 24 X 7 X 365 on offer.

IIZUKA's standard SLA is below:

Our standard SLA is set-out below. Variance to triggers and response times can be accommodated if reasonable

Severity Level 1 Failure of business critical function

Response 30 mins

Target Resolution 4 hours

- Main business use interruption (e.g. unable to process cases or to run report at month end)
- Apparent loss of business critical data

Severity Level 2 Defect in high usage function

Response 30 mins

Target Resolution 16 hours

- Functional error preventing use of specific screen within a case (e.g. unable to record notes)

Severity Level 3 Defect in low usage function

IIZUKA Response to LCMS Requirements ITT
Response 30 mins

Target Resolution 40 hours

- Search returning incorrect results
- Failure to send reminder emails

Severity Level 4 Non-functional defect

Response 30 mins

Target Resolution by agreement

- Inconsistent sorting
- Unintended process outcome
- Typographical or layout error

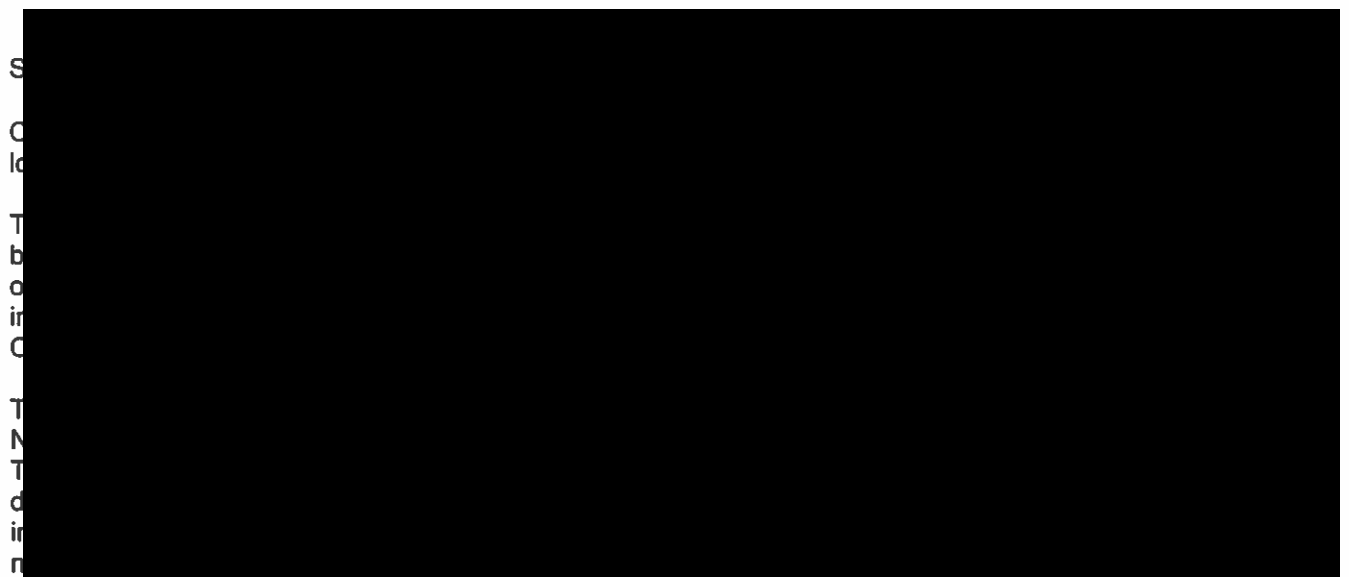
Have you provided any similar/existing case management systems in the legal field/public sector? If so, how long ago?

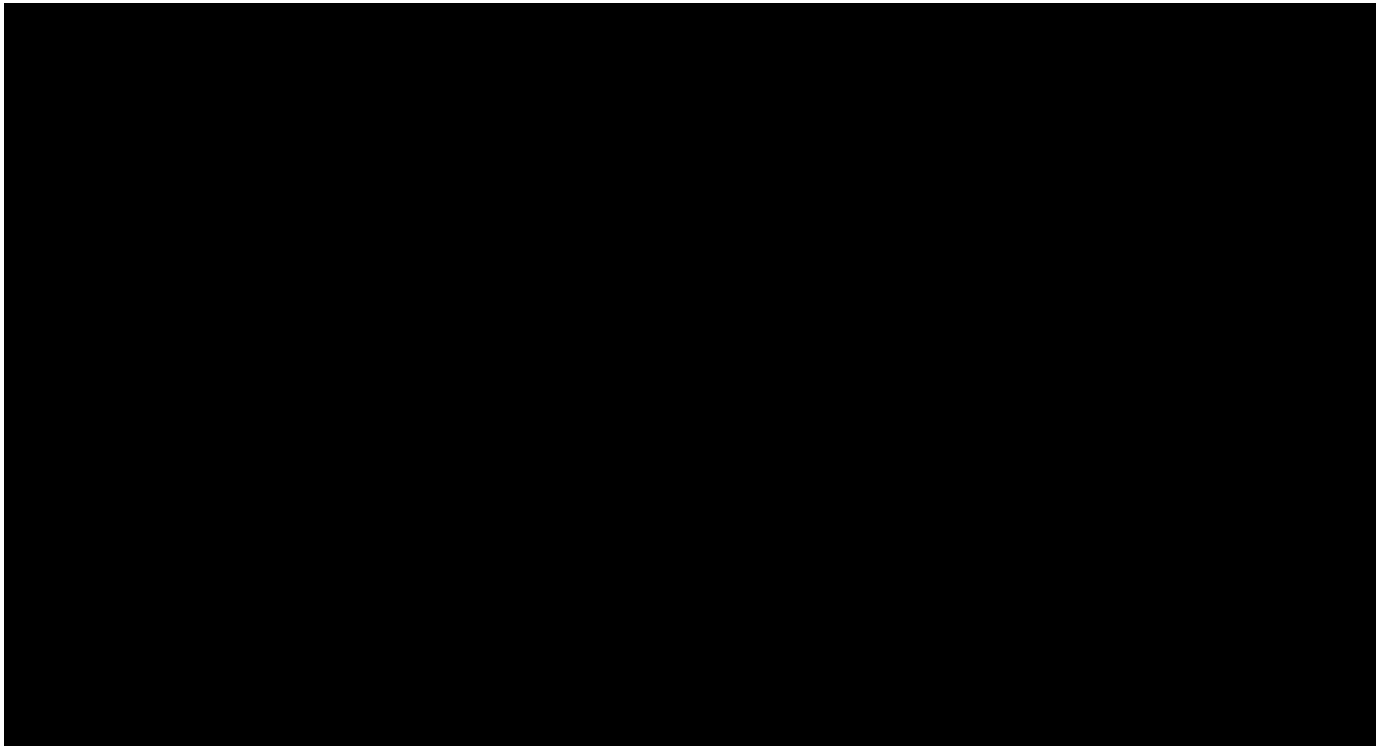
IIZUKA has been providing secure Case Management for 15+ years to UK public and 3rd sectors. It's all we do and it's all we've ever done. Case Manager® is used by organisations both large and small to manage their complex, long-term interactions with their clients and all predominantly within highly regulated environments where robust, secure systems are essential tools that help to provide compliance and governance.

Case Manager® is used in the following areas:

- Central Government
- Local Government
- NGB's
- Police
- Education
- Housing
- Health
- Charities

Some recent examples of our work:





Given this contract is relatively short (12 months) please explain the exit/off boarding process and when would this process commence (in particular how is our information packaged and delivered to us as part of the exit or off boarding strategy)?

The data in Case Manager is held in a relational database that is integral to the operation of Case Manager and is of limited use to the CQC in that form without an instance of Case Manager through which it can be navigated. The Off-Boarding process will therefore create an extract of the information that CQC can take and import into an alternative solution. As the data is relational there are multiple dimensions to the data and it therefore does not lend itself to flattening into a single data file. Instead IIZUKA will export the system as a nested XML structure or as a series of text/CSV files containing different sets of records. Attachments and documents will be extracted as files and bundled into a zip archive, with individual files having a file path that contains the unique id of the record to which they should be attached.

The data extracted will include the data from the case records including people, notes, actions etc, but will not contain peripheral configuration data, copies of the audit logs or any other information that is relevant only to the operation of the Case Manager solution.

The full set of data will be provided on an encrypted USB drive and handed to a nominated CQC member of staff.

Preparation for this process will begin during the final month of the contract with the final extract being created within two weeks of the end of the contract.

Appendix I - Information Management Principals Response

Suppliers to confirm that the tool being proposed is able to operate in line with the above principles.

Plan

The implementation of Case Manager will provide the CQC with a new location in which to store data. This is an improvement over the current practice where documents are held only in shared folders. By using Case Manager the CQC will have the ability to define clear management information practices and rules in relation to the storage of cases and related documents and personal information.

During the requirements analysis phase of the project IIZUKA will liaise with the CQC to determine the types of information to be held and their associated levels of sensitivity. The Case Manager system will then be configured so as to guide the users in what to record and when and will automatically associate appropriate security permissions to those records using agreed business rules.

Share

Information is held in Case Manager in a fully relational system that ensures records are only created once and are linked to related records, instead of being duplicated. This ensures that users are acting on the most up to date information and that stale or incorrect information is not maintained.

Case Manager includes a comprehensive Role Based Access Model (RBAC) that allows access to information and to functions on a role, team, organisation or individual basis. This means that data can be held once but can be securely shared with authorised users with a defined level of granularity.

Information held in Case Manager is clearly structured and follows a strong and consistent information architecture. This means users are aware of what the data means and is for. The structure also provides guidance and a framework that assists the user in determining what information needs to be captured and what doesn't.

Protect

Case Manager provides a strong, rule based framework in which to record information. Users are guided in the information that they record, through structured fields and on screen guidance. Once captured, information is securely held and protected with a comprehensive RBAC model.

The relational database structure ensures that interrelated data refers to single copies of data and that diverging duplicates are not created. This means that when updates or corrections are made they apply immediately across the system and are visible from all related records accordingly.

Case Manager allows access to records to be controlled by both rules and at the individual record level. This ensures that consistency is maintained, but also so that specific records can be restricted further when required.

Case Manager provides a mechanism for automatically deleting or anonymising data after it is no longer needed. This is configurable to meet the CQC data protection policies.

Maintain

Case Manager's structure provides assistance to users in helping them record information correctly. Data fields are strongly typed to ensure that users enter valid data, for example dates, numbers, prices etc.. Mandatory fields are also enforced so that users must enter information that is considered vital to the business's processes. Control over these fields and their mandatory behaviour is granted to authorised administrators who can ensure that only the minimum number of fields are made mandatory. Case Manager's inbuilt management information reporting tools, workflow, case review and quality control features all provide means through which the business is able to monitor and maintain its data quality.

As described above, Case Manager is configured to automatically delete or anonymise data when it passes its scheduled retention period.

Schedule 2 - Call-Off Contract charges

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

- 60 user licence for Case Manager
- Service Management
- Training.

Part B - Terms and conditions

1. Call-Off Contract start date and length

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.2 to 5.3 (Force majeure)
- 5.6 (Continuing rights)
- 5.7 to 5.9 (Change of control)
- 5.10 (Fraud)
- 5.11 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)

- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

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

- 2.3 The Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.
- 2.4 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

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

4. Supplier staff

- 4.2 The Supplier Staff must:

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

- 4.3 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.

- 4.4 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.5 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.
- 4.6 The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
- 4.7 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.8 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.
- 4.9 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - have raised all due diligence questions before signing the Call-Off Contract

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

6. Business continuity and disaster recovery

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

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

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

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

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

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

- a broker's verification of insurance

- receipts for the insurance premium
- evidence of payment of the latest premiums due

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

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.83 to 8.91. The

indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
- rights granted to the Buyer under this Call-Off Contract
 - Supplier's performance of the Services
 - use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

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

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

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

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

12. Protection of information

12.1 The Supplier must:

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

- 12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
- providing the Buyer with full details of the complaint or request
 - complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
 - providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
 - providing the Buyer with any information requested by the Data Subject
- 12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

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

- 13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policy and all Buyer requirements in the Order Form.
- 13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

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

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

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

- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

16.5 The Supplier will immediately notify CCS of any breach of security of CCS's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the

breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:
- an executed Guarantee in the form at Schedule 5
 - a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

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

- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
 - any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
- the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
 - an Insolvency Event of the other Party happens
 - the other Party ceases or threatens to cease to carry on the whole or any material part of its business
- 18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
- 18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

- 19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.
- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- any rights, remedies or obligations accrued before its Ending or expiration
 - the right of either Party to recover any amount outstanding at the time of Ending or expiry
 - the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data); 19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)
 - any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires
- 19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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

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

20. Notices

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

Manner of delivery	Deemed time of delivery	Proof of service
--------------------	-------------------------	------------------

Email	9am on the first Working Day after sending	Sent by PDF to the correct email address without getting an error message
-------	--	---

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

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

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

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

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

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

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data

- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

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

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

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

23. Force majeure

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

24. Liability

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

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

25. Premises

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

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

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

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

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

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

- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer

- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

32. Variation process

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

- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

- 33.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only Processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional Processing if permitted by Law).
- 33.2 The Supplier will assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation before commencing any Processing (including provision of detailed information and assessments in relation to Processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.
- 33.3 The Supplier must have in place Protective Measures, details of which shall be provided to the Buyer on request, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.
- 33.4 The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier staff with access to Personal Data, including by ensuring they:
- i) are aware of and comply with the Supplier's obligations under this Clause;
 - ii) are subject to appropriate confidentiality undertakings with the Supplier

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

- 33.5 The Supplier will not transfer Personal Data outside of the European Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.
- 33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.
- 33.7 The Supplier will notify the Buyer without undue delay if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation, and insofar as this is possible, in accordance with any timescales reasonably required by the Buyer
- 33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
- i) the Buyer determines that the Processing is not occasional;
 - ii) the Buyer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

iii) the Buyer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Call-Off Contract, the Supplier must:

- i. notify the Buyer in writing of the proposed Sub-processor(s) and obtain its written consent;
- ii. ensure that it has entered into a written agreement with the Sub-processor(s) which gives effect to obligations set out in this Clause 33 such that they apply to the Sub-processor(s); and
- iii. inform the Buyer of any additions to, or replacements of the notified Sub-processors and the Buyer shall either i) provide its written consent or ii) object.

33.10 The Buyer may at any time put forward a Variation request to amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement

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

Schedule 4 - Alternative clauses

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

Schedule 5 - Guarantee

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

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none">● 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	<p>Data, personal data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> ● 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 Data Protection Legislation.
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	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed

Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.
Data Protection Legislation	<p>Data Protection Legislation means:</p> <ul style="list-style-type: none"> i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; iii) all applicable Law about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Takes the meaning given in the Data Protection Legislation.
Default	<p>Default is any:</p> <ul style="list-style-type: none"> ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for

	Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: <ul style="list-style-type: none"> ● acts, events or omissions beyond the reasonable control of the affected Party

	<ul style="list-style-type: none"> ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> ● 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 RM1557.10 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or

	at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FOIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	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.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government guidance and the Crown Commercial Service guidance, current UK Government guidance will take precedence.
Indicative Test	ESI tool completed by contractors on their own behalf at the

	request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: <ul style="list-style-type: none"> ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: <ul style="list-style-type: none"> ● 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:

	<ul style="list-style-type: none"> ● the supplier's own limited company ● a service or a personal service company ● a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR Claim	A claim as set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in

	contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.

Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity

	<ul style="list-style-type: none"> ● commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising 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).
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend Controls	The approval process used by a central government Buyer if it

	needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
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 - Processing, Personal Data and Data Subjects

Subject matter of the processing:



Legal Case Management System

Duration of the processing:



Duration of the contract –

Nature and purposes of the Processing:

All documentation relating to legal cases will be stored in the system. Case data includes full case history including personal details, notes, correspondence, case actions, images.

This information will be obtained as it currently is from internal CQC employees seeking legal advice and support, as well as any legal matters and challenges that are brought to CQC's attention by external parties. The legal case management system is only accessible to CQC Legal staff. There will be no transfer of information out of the system, except where required to respond to legal cases.

Type of Personal Data:



CQC staff contact details ie telephone numbers and email addresses

External solicitors / counsel contact details ie name, address, telephone numbers and email addresses

Personal details of service users, staff, providers. Photographic images of service users could be used as evidence

Client contact details ie name, address, telephone numbers and email addresses

Provider/location details

Categories of Data Subject:



CQC staff contact details

Provider names and locations, including names of individuals.

Personal details of patients, staff and others associated with cases.

Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data:

The information stored on the server and cloud based system will adhere to the KIM retention and disposal schedule as there will be a functionality within the LCMS that has a date and time calculator of how long the information has been retained for so that when the time comes, the information can be disposed of.

The retention schedule for all CQC information is held by the KIM teams. The information stored and the duration will be reflected on the asset register, which is held by KIM colleagues.

During the last month of the contract CQC will work with iizuka Software Technologies to implement the off boarding and exit strategy to extract the data ready to import into an alternative system

Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data:



The information stored on the server and cloud based system will adhere to the KIM retention and disposal schedule as there will be a functionality within the LCMS that has a date and time calculator of how long the information has been retained for so that when the time comes, the information can be disposed of.

The retention schedule for all CQC information is held by the KIM teams. The information stored and the duration will be reflected on the asset register, which is held by KIM colleagues.

During the last month of the contract CQC will work with iizuka Software Technologies to implement the off boarding and exit strategy to extract the data ready to import into an alternative system