Crown
Commercial
Service

G-CLOUD 8 CALL-OFF CONTRACT

PROVISION OF A LEGAL CASE MANAGEMENT SYSTEM

This Call-Off Contract for the G-Cloud 8 Framework Agreement (RM1557viii) includes:

Part A - Order Form

Buyer	Care Quality Commission
Service reference	267479360522966
Supplier	IIZUKA Software Technologies
Call-Off Contract ref.	CQC ICTC 556
Call-Off Contract title	Legal Case Management System r
G-Cloud Framework No.	G Cloud 8
Call-Off Contract description	The provision to supply, support and implement a legal case management system
Start date	5 April 2017
End date	4 April 2018 (option to extend for a further 12 months)
Call-Off Contract value	£130,800 Including VAT
Charging method	Payment will be made in instalments in-line with the payment milestones articulated within this Order Form and upon satisfactory completion of the deliverables.
Purchase order No.	TBC

This Order Form is issued in accordance with the G-Cloud 8 Framework Agreement (RM1557viii).

This Order Form may be used by Buyers to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any supplementary terms that materially change the Deliverables offered by the Supplier and defined in the Tender documents, such as the Service Definition and the Supplier Terms.

There are terms within the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with the use of square brackets e.g. "[this is a term you can alter]".

Project reference:	**CQC ICTC 556**
Buyer reference:	CQC ICTC 556
Order date:	04/04/2017
Purchase order:	TBC
From: the Buyer	Buyer's name: Care Quality Commission Buyer's address: Care Quality Commission, 3rd Floor 151 Buckingham Palace Road, London, SW1W 9AZ
To: the Supplier	Supplier's name: IIZUKA Software Technologies Limited Supplier phone:0121 200 8906 Supplier's address: Unit 106 - 206 The Argent Centre 60 Frederick Street Birmingham B1 3HS Company number: 4498601
Together:	**the "Parties"**

Principle contact details

For the Buyer:	Name & title:	[redacted]
	Email:	[redacted]
	Name & title:	[redacted]
	Phone:	03000 616161
For the supplier	Name & title:	[redacted]
	Email:	
	Phone:	

Call-off contract term

Commencement date:	This Call-Off Contract commences on 5th April 2017 and is valid for 12 months (4th April 2018) with the option to extend for periods up to a further 12 months (ending 4th April 2019).
Termination:	In accordance with Call-Off Contract clause 23 the notice period

required for Termination is at least 30 days from the date of written notice for disputed sums or at least 30 days from the date of written notice for termination without cause.

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 utilized by Buyer may vary from time to time during the course of this Call-Off Contract, subject always to the terms of the Call-Off Contract.

G-Cloud 8 Lot

This Call-Off Contract is for the provision of Services under
Lot 3 SaaS Software as a Service

G-Cloud 8 services required:

The Services to be provided by the Supplier under the above Lot are listed in Schedule 1 and outlined below:

- 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

To support the above, the Supplier will be required to deliver the following Contract Service Deliverables outlined in Table 1 which comprise key Contract Milestones:

Table 1: Key Contract Milestones (Deliverables):

Description	Target Date (to be decided	Action to achieve Milestone	Review Date
Milestone 1:			
Project Initiation Meeting (PIM)	April-17	Project Initiation Meeting- takes place	April-17
Draft Requirement Specification	April -17	Draft Requirement complete	April-17
Arrange workshop schedule x 8	April/May -17	Workshop schedule arranged x 8 [redacted]	April/May 17
Prototype system delivery	April/May -17	Prototype system delivered [redacted]	April/May -17
Milestone 2			
Infrastructure sandbox delivery	April/May -17	Infrastructure sandbox delivered Hosting [redacted]	May-17
Complete workshop delivery	May-17	Complete workshop delivery [redacted]	May -17
Finalise requirements specification and sign-off	May-17	Finalise requirements specification write up and signed-off [redacted]	May-17

Milestone 3:			
Build and configure prototype system	June-17	Prototype System built & test [redacted]	Mid-June-17
Milestone 4:			
User acceptance testing and Training	July-17	User acceptance testing and Training complete [redacted]	Mid-July 17
Milestone 5:			
Handover to business as usual team (BAU) Licence finalisation Go-live	Aug-17	BAU handed over [redacted]	Mid Aug-17

The Supplier will be expected to satisfy the following Key Performance Indicators (KPI's) detailed within Table 2 as part of Service Delivery:

Indicator	Measured by	Review date/
System availability	99.5% uptime	Quarterly
Page response times	>2 seconds	Quarterly

Additional Services:

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

Location:	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 spent by the Supplier at the Buyer's Head Office (151 Buckingham Palace Road, London) and possibly at CQC other offices (i.e. Newcastle, Leeds) in order to understand, support and work with the Buyer's project team
Quality standards:	The quality standards required for this Call-Off Contract are ISO:27001 and ISO:9001and CESG
Technical standards	The technical standards required for this Call-Off Contract are N/A
On-boarding	The on-boarding plan for this Call-Off Contract is that an initial implementation meeting will occur upon Contract commencement between the Buyer and the Supplier. The Supplier will be expected to deploy the appropriate resource to facilitate delivery of the Services Deliverables/ Milestones
Off-boarding	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
Limit on supplier's liability:	In accordance with Call-Off Contract clause 31.5, the Limit on supplier's liability for direct loss, destruction, corruption, degradation or damage to the Buyer Data or the Buyer Personal Data or any copy of such Buyer Data is £500,000.00
Insurance:	In accordance with Call-Off Contract clause 10, the insurance(s) required will be: a minimum insurance period of 6 years following the expiration or earlier termination of this Call-Off Contract professional indemnity insurance cover to be held by the Supplier and by any agent, Sub-Contractor 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 such higher limit as the Buyer may reasonably require (and as required by Law) employers' liability insurance with a minimum limit of £5,000,000 or

such higher minimum limit as required by Law from time to time.

Buyer's Responsibilities	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.
Buyer's equipment	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

Commercially sensitive information:	The following is a list of the Supplier's commercially sensitive information Code Base, pricing.
Subcontractors / Partners:	The following is a list of the Supplier's Subcontractors/Partners Rackspace, E-Studi.

Call-Off Contract Charges and payment

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

Payment method (GPC or BACS):	The method of payment for this Call-Off Contract is BACS
Payment profile:	The payment profile for this Call-Off Contract is to be made in instalments in-line with completion of the following Contract Service Deliverables/ Milestones (taken from Table 1 of the Order Form) Milestone 1. [redacted] on satisfactory completion of and acceptance of prototype license and 8 x workshop delivery. Completed by 30/05/2017 Milestone 2. [redacted] workshop finalisation, specification write up £2,850 on satisfactory completion of acceptance of above Completed by 30/05/2017 Milestone 3. [redacted] on satisfactory completion of acceptance of

	prototype system built and test Completed by 30/06/2017 Milestone 4. [redacted] on satisfactory completion of acceptance of user acceptance testing and training Completed by 31/07/2017 Milestone 5. [redacted] n satisfactory completion of acceptance of handover to BAU team and license finalisation completed by 31/08/2017
Invoice details:	The Supplier shall issue an electronic invoice in-line with the above payment method in arrears. In accordance with Call-Off Contract clause 8, the Buyer will pay the Supplier within 30 calendar days of receipt of a valid invoice
Who and where to send invoices to:	Invoices shall be sent to Care Quality Commission T70 Payables F175, Phoenix House, Topcliffe Lane Wakefield, West Yorkshire, WF3 1WE.
Invoice information required – eg PO, project ref, etc.	All invoices must include a PO number (to be supplied by the Buyer), date and Contract reference number.
Invoice frequency	Invoice will be sent to the Buyer upon satisfactory completion of the Service deliverables in-line with the payment milestones
Call-Off Contract value:	The value of this Call-Off Contract is £130,800 Including VAT.
Call-Off Contract Charges:	The total Call-Off Contract value of 130,800 Including VAT is to be paid in-line upon completion of the payment milestones listed above.

Additional Buyer terms

This Call-Off Contract will include the following Contract deliverables/milestone (also detailed within Table 1 of this Order Form): This Call-Off Contract will include the following Contract deliverables/milestone (also detailed within Table 1 of this Order Form):

Performance of the service and deliverables	This Call-Off Contract will include the following implementation plan and milestones: • Implementation plan to be completed and finalised 30 days after contract award.
Collaboration agreement	The Buyer does not require the Supplier to enter into a Collaboration Agreement. [In addition to its obligations under any Call-Off Contract, the Supplier shall: • work pro-actively with each of the Buyer's contractors • cooperate with the Buyer's contractors of other services to enable the efficient operation of the ICT services, and • assist in sharing information with the Buyer's contractors for the purposes of facilitating adequate provision of the G-Cloud Services
Warranties, representations	In accordance with Call-Off Contract clause 6, the Supplier warrants and represents to the Buyer that enter any additional warranties and representations.
Supplemental requirements in addition to the call-off terms	In accordance with Call-Off Contract clauses, the Supplier will N/A.
Buyer specific amendments to/refinements of the Call-Off Contract terms	In accordance with Call-Off Contract clauses, the Supplier will N/A.
Public Services Network (PSN)	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources. If the required G-Cloud Services are to be delivered over the Public Services Network this should be detailed in the Call-Off Contract Order Form. **Delivery of PSN Compliant Services** If requested to do so by the Buyer, the Supplier shall ensure that the G-Cloud Services adhere to the conditions and obligations

identified in the PSN Code of Practice at the Supplier's cost.

If any PSN Services are Sub-Contracted by the Supplier, the Supplier must ensure that services have the relevant PSN compliance certification, which includes:

- Buyer environments
- communications components
- compliant and certified

Role of the PSN authority

The Supplier will immediately disconnect its G-Cloud Services from the PSN if instructed to do so by the PSN Authority following an event affecting national security, or the security of the PSN. The Supplier agrees that the PSN Authority shall not be liable for any actions, damages, costs, and any other liabilities which may arise as a consequence.

- This clause may be enforced by the PSN Authority, notwithstanding the fact that the PSN Authority is not a party to this Call-Off Contract.

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 In accordance with the Buying process set out in the Framework Agreement, this Call-Off Contract will be formed when the Buyer acknowledges the receipt of the signed copy of the Order Form from the Supplier.

1.4 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 undertook to provide such Services under the terms set out in Framework Agreement number RM1557viii (the "Framework Agreement").

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

SIGNED:

	Supplier:	**Buyer:**
Name:	[redacted]	
Title:		

Signature:	[redacted]
Date:	4/

Part B - The Schedules

Schedule 1 - Buyer's Requirements and Contract Deliverables

Appendix A - Overview of Legal Case Management System

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") 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 77 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;
2. Adult Social Care;
3. Primary Medical Services, Hospitals and Registration;
4. Corporate Governance and Employment;
5. Procurement and Contracts;
6. Information Rights;
7. Ratings Review; and
8. National Complaints

(See Appendix 2 for detailed description)

1.7. CQC is seeking 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 is necessary to enable delivery of an effective in house legal service that includes 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 recent Law Society compliance assessment.

1.9. It is 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. The GLS presently operates using primarily manual business systems with very little in terms of technological solutions supporting their processes. This results in an inability to effectively track and monitor workloads of staff or specific cases as it is not capable of supporting effective case management of civil or criminal litigation. Cases involving court deadlines and large volumes of disclosure 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 also move with the times.

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. At present, we do not have a digital case management system and are therefore unable 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 seeks to procure software as a service a legal case management system for initially 12 months with an option to extend for up to a further 12 months.

2.2. It is envisaged that the system will be licensed for up to 60 users and training will be required as part of the implementation.

3. THE REQUIREMENT

3.1. The GLS Team currently operates using primarily manual business systems with very little in terms of technological solutions supporting their processes. This results in an inability to effectively track and monitor workloads of staff or specific cases. GLS staff currently saves all legal documents, correspondence through Y: drive (Windows Explorer) and this is restrictive as we have to seek permission to open new folders thereby slowing the system for retrieval and storage of documents. Legal Advisors spend lots of time searching for cases and in many instances and cannot ascertain what a colleague's last actions were on a case, thus making it difficult for another colleague to take over the case, this results in inconsistencies with the legal services being provided.

3.2. The GLS Team does not have a way of recording time spent on completing particular areas of legal work for both internal and external Legal Advisors in order to successfully verify and recover cost incurred in providing legal services.

3.3. A case management system will enable legal cases to be better managed. It will make 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.

3.4. 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.

3.5. System Users

- Senior Management Team [6]
- Legal Managers [3]
- Principal Legal Advisors [15]
- Senior Legal Advisors [12]
- Legal Advisors [9]
- Paralegals [5]
- Business Support [4]
- Complaints Team [10]
- Ratings Review Team [6]
- Information Governance Team [7]

3.6. Matters per year (analysis of 2015-2016 figures)

- Litigation
  - 140 Prosecution cases
  - 120 First Tier Tribunal cases
  - 108 Inquests
  - 5 Legal Challenges
- Contracts and Procurement (including Health Watch England and other Commercial matters)
  - 78 cases
- Adult Social Care cases
  - 1680 cases
- Primary Medical Services. Hospitals and Registration cases
  - 1,440 cases
- Civil Litigation
  - Size (per bundle) Upper Tier 100- 200 pages
  - Size (per bundle) First Tier Tribunal 300-500 pages
  - Litigation cases have multiple bundles (6)
  - High Court – Judicial Review cases - 300-500 pages
  - Magistrates' Court – Prosecution cases - 600-1000 pages

3.7. The main objectives are 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

3.8. In order to meet these key objectives, the following have provisionally been identified as key benefits and features that the Legal Case Management system will provide for the user:

- 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)

3.9. Business Support

3.9.1. 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.

3.10. Training

3.10.1. 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 the initial sessions to be facilitated by the successful supplier with training to be updated thereafter internally and/or externally as the needs of GLS develop with CQC. Again this will be dependent on how much custom development would be needed of the chosen legal case management system

3.10.2. Initial support and ongoing support will be dependent on what system is available to meet GLS's business needs.

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

3.10.4. A role specific training programme will initially be required for approximately 55 legal staff which includes Paralegals, Principal Legal Advisors; Senior Legal Advisors and Legal Managers. A further training programme may also be required for other members such as Complaints and the Ratings Team.

3.10.5. Separate Training programme for Managers on Reporting, producing time reports, audit trails, Case progression reports.

3.10.6. Separate Training on how to create bespoke requests for Information, re FOI requests and how to search the new case management system to obtain this data.

4.

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 Level Requirement	**Description – Functional Requirements**
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) • **[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-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) • **[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 • **[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 overseen by the manager is saved to the right case (MUST) • **[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-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) • **[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 prioritize 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	• **[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 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). •
Tasks, Templates and Prompts	• **[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 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	• **[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 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 Status) (MUST) • **[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 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	• **[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 (QRAM- QUALITY REVIEW ASSURANCE MANAGEMENT). • **[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-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) • **[SCM-68]** As a User, I want to have the ability to archive cases, so that I can comply with legislation (MUST) • **[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 Data protection Act 1998 • **[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	• **[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

Cost & Fees	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	• **[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	• **[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 • **[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 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 above, making use of CQC's Mulesoft 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.
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 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. 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 Data Protection Act (1998), 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 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.

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.
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 be 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.
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 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.
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 lockout 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 Data Protection Act (1998), 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. Information Management Principles

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

Microsoft Word 97 - 2003 Document

8. Architectural Principles

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

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

Microsoft Word 97 - 2003 Document

9 Authority Responsibilities

- Legal Services to appoint a project lead to oversee the work and liaise with / report to supplier contract manager.

10 Contractor Responsibilities

- Appoint a contract manager to oversee the work and liaise with / report to CQC's project lead.
- Provide weekly updates of progress (the format of reporting will be agreed at the outset of the contract between the selected supplier and CQC, but it should cover overall progress against plan, risks to plan and mitigating actions, issues and escalations and project budget tracking).
- Perform quality assurance on all aspects of the programme.
- Provide confirmation that they are managing within the agreed total costs for the project as part of progress updates.

11 Contract Management and Monitoring

KPIs to be applied to this contract are:

- The timeliness of deliverables against key dates
- Regular progress reports (weekly)
- Working effectively in conjunction with CQC Legal Services project lead
- The selected supplier will be expected to attend a post contract review to consider whether the objectives of the contract were met; to review the benefits achieved; and to identify any lessons learnt for future developments of the system
- Testing of system
- Training sessions for users
- After care support

12 Timetable

- Design to be completed by dates to be agreed
- Implementation of system by dates to be agreed
- Testing of system by dates to be agreed
- Go live prior to or by 31st March 2017

13 Skills and Knowledge Transfer

The selected supplier will work closely with CQC's Legal team to ensure the system is designed in line with business needs.

Significant training and guidance required for all staff.

14 Further Information

The procurement of a case management system is to a limited budget. To minimise costs the selected supplier should consider as far as possible opportunities for joint working with CQC.

15 EVALUATION

	EVALUATION CRITERIA & QUESTIONS		WEIGHT
1	**QUALITY**		**60%**
1.1	**Overview** Please provide a concise summary highlighting the key aspects of the G Cloud offering for a legal case management system. This response must not exceed 3 pages of A4 Ariel 12 Text.		5%
1.2	**Technical Merit & Functional Business Requirements** • Describe with specific reference to functional requirements how it is intended to deliver the solution that meets these requirements as included in the statement of requirements. Clearly describe where a requirement is met, not met or partly met for functional requirements. • 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? This response must not exceed 4 pages of A4 Ariel 12 Text.		20%
1.3	**Technical Merit for Non Functional Requirements – Generic SaaS** • Describe with specific reference to non-functional and security requirements how it is intended to deliver the solution that meets these requirements as included in the statement of requirements. Clearly describe where a requirement is met, not met or partly met for both non-functional and security requirements. • 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. • Describe the identification and authentication procedures and protocols to be used and any supported federation mechanisms available. This response must not exceed 4 pages of A4 Ariel 12 Text.		15%

1.4	**Technical Merit for Non Functional Information Security** • Describe with specific reference to non-functional Information security requirements how it is intended to deliver the solution that meets these requirements as included in the statement of requirements. Clearly describe where a requirement is met, not met or partly met for both non-functional and security requirements. • Data purging/archiving – What is your data retention policy? This response must not exceed 4 pages of A4 Ariel 12 Text.		10%
1.5	**Technical Merit for CQC Technical Architecture principals** • Describe with specific reference the technical architecture principals how it is intended to deliver the solution that meets the architecture principals. • 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. This response must not exceed 4 pages of A4 Ariel 12 Text.		15%
1.6	**Service Delivery** • 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? • Have you provided any similar/existing case management systems in the legal field/public sector? If so, how long ago? This response must not exceed 4 pages of A4 Ariel 12 Text.		10%
1.7	**Exit/Off Boarding** • 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)? This response must not exceed 3 pages of A4 Ariel 12 Text.		5%
1.8	**Demonstration** • Suppliers must provide a demonstration of their Legal Case Management System demonstrating the end to end process. This will be assessed against the scoring criteria looking at usability, minimum amount of changes. 10% • Suppliers must provide an outline transition implementation plan to indicate its plans for the transition from contract award into the new contract delivery phase. 10% *This criterion will be determined through demonstration and is not required for the submission of the response. Suppliers will be expected to bring a written account to the demonstration.* *Any supplier whose submission scores 1 or below in any of the criteria will result (at CQC's sole discretion) in that submission not being taken forward or considered further to the demonstration stage.*		20%

2	PRICE		40%
2.1	**Financial** Cost of solution including whole life, support, individual licences, controlled changes and any integration costs, training etc. *This will be assessed by the maximum points will be awarded to the lowest price and all other scores will be awarded in direct inverse proportion.*		100%

Tenders will be scored using the following scoring model:

Table 1 : Scoring Scheme

GRADE LABEL	GRADE	DEFINITION OF GRADE
Unacceptable	0	The response has been omitted, or the Tenderer proposal evidences inadequate (or insufficient) delivery of the requirement
Weak	1	The Tenderer proposal has merit, although there is weakness (or inconsistency) as to the full satisfaction of the delivery requirement
Satisfactory	2	The Tenderer proposal has a suitable level of detail to assure that a satisfactory delivery of the service requirement is likely.
Good	3	The Tenderer proposal has evidenced a level of understanding that assures there will be desirable value-add within the solution **or** superior and desirable (time or quality) delivery outcomes.
Excellent	4	The Tenderer proposal evidences significant levels of understanding **and** offers an **innovative** solution that includes desirable value-add to the Authority.

All suppliers are to note -
Any supplier whose submission scores 1 or below in any of the criteria will result (at CQC's sole discretion) in that submission not being taken forward or considered further to the demonstration stage.

Schedule 1b- Supplier's Response to Requirements

Please see Annex A Supplier's response to requirements

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) cannot be amended during the term of the Call-Off Contract. The detailed breakdown for the provision of Services during the term of will include (but will not be limited to):

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

Schedule 3 - Deed of guarantee

Not used

Schedule 4 - Alternative Clauses

Not used

Part C – Terms and conditions

1. Call-Off Contract start date, length and methodology

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

1.2 This Call-Off Contract will terminate on the End Date specified in the Order Form unless terminated earlier in accordance with Clause 23 and will be a maximum of 24 months from the Commencement Date.

2. Overriding provisions

2.1 The Supplier agrees to supply the G-Cloud Services [and any Additional Services (Lot 4 only)] in accordance with this Call-Off Contract and the Supplier's Terms as identified in the Framework Agreement (G-Cloud Services) and incorporated into this Call-Off Contract.

2.2 In the event of and only to the extent of any conflict or ambiguity between the Clauses of this Call-Off Contract, the provisions of the Schedules, any document referred to in the Clauses of this Call-Off Contract (including Supplier's Terms) and the Framework Agreement, the conflict shall be resolved in accordance with the following order of precedence:

- the Framework Agreement
- the Clauses of this Call-Off Contract (excluding Supplier Terms)

- the completed Order Form
- the Supplier's Terms and Conditions, and
- any other document referred to in the Clauses of this Call-Off Contract.

The Supplier accepts this is the order of prevailing provisions in this Call-Off Contract.

3. Transfer and sub-contracting

3.1 The Supplier will not assign, novate or sub-contract any part-of this Call-Off Contract without the Buyer's prior written approval which shall not be unreasonably withheld or delayed.

3.2 The Supplier will be responsible for the performance of any Sub-Contractors.

3.3 The Buyer may assign, novate or otherwise dispose of its rights and obligations under this Call-Off Contract or any part thereof to:

- any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Buyer, or
- any private sector body which substantially performs the functions of the Buyer

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under this Call-Off Contract.

4. Supplier Staff

4.1 The Supplier Staff will:

- fulfil all reasonable requests of the Buyer
- apply all due skill, care and diligence to the provisions of the Services
- be appropriately experienced, qualified and trained to supply the Services
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary vetting procedures specified by the Buyer
- Comply with the provisions of the Official Secrets Act 1911 to 1989; and
- Section 182 of the Finance Act 1989.

5. Due diligence

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

5.2.1 having made their own enquiries are satisfied by the accuracy of any information supplied by the other Party

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

5.2.3 have entered into this Call-Off Contract relying on their own due diligence

6. Warranties, representations and acceptance criteria

6.1 The Supplier will perform its obligations under this Call-Off Contract with all reasonable care, skill and diligence, according to Good Industry Practice.

6.2 The Supplier will use all reasonable endeavours to prevent the introduction, creation or propagation of any disruptive elements into systems providing services to data, software or Authority Confidential Information held in electronic form.

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

6.4 The Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions and Intellectual Property Rights to perform this Call-Off Contract.

6.5 The Supplier represents that, in entering into this Call-Off Contract it has not committed any Fraud.

6.6 The Supplier undertakes to pay all taxes due from it to HMRC and will not indulge in "disguised employment" practices when delivering services under this Call-Off Contract, and

6.7 For the avoidance of doubt, the fact that any provision within this Call-Off Contract is expressed as a warranty shall not preclude any right of termination the Buyer may have in respect of breach of that provision by the Supplier.

7. Business continuity and disaster recovery

7.1 The Supplier will ensure a disaster recovery approach is captured in a clear disaster recovery plan contained within their service descriptions where appropriate and required by the Buyer.

8. Payment terms and VAT

8.1 The Buyer will pay the Supplier within 30 days of receipt of a valid invoice submitted by the Supplier in accordance with this Call-Off Contract.

8.2 The Call-Off Contract Charges are deemed to include all Charges for payment processing. All Invoices submitted to the Buyer for the Services shall be exclusive of any Management Charge.

8.3 All charges payable by the Buyer to the Supplier shall include VAT at the appropriate rate.

8.4 The Supplier will add VAT to the charges at the appropriate rate.

8.5 Where specified within 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 shall not recover this charge from the Buyer.

8.6 The Supplier will ensure that each invoice contains all appropriate references and a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

8.7 Supplier Sub-Contracts must oblige the Supplier to make payments to its Sub-Contractor within 30 calendar days from the receipt of a valid invoice.

8.8 The Supplier shall 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 shall pay all monies pursuant to this indemnity to the Buyer not less than 5 UK working days before the date upon which the tax or other liability is payable by the Buyer.

8.9 The Supplier shall not suspend the supply of the G-Cloud Services for Buyer's failure to pay undisputed sums of money unless the Supplier is entitled to suspend or terminate this Call-Off Contract. Interest shall be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

8.10 In the event of a disputed invoice, the Buyer shall make payment in respect of any undisputed amount in accordance with the provisions of this Call-Off Contract and return the invoice to the Supplier within 10 UK working days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The Supplier shall respond within 10 UK working days of receipt of the returned invoice stating whether or not the Supplier accepts the Buyer's proposed amendments. If it does then the Supplier shall supply with the response a replacement valid invoice.

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

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

10. Insurance

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

10.1 Subcontractors

10.1.1 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 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.

10.2 Agents and professional consultants

10.2.1 The Supplier will also ensure that all agents and professional consultants involved in the supply of 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 termination or expiry date to this Call-Off Contract to which the insurance relates.

10.2.2 The Supplier will also ensure that all agents and professional consultants involved in the supply of Services hold employers liability insurance to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the termination or expiry date to this Call-Off Contract to which the insurance relates.

10.3 Additional or extended insurance

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

10.3.2 The Supplier will provide CCS and the Buyer with the following evidence that they have complied with clause 10.3.1 above:

- a broker's verification of insurance; or
- receipts in respect of the insurance premium; or
- other evidence of payment of the latest premiums due.

10.4 Supplier liabilities

10.4.1 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract.

10.4.2 The Supplier will:

- take all risk control measures relating to the Services as it would be reasonable to expect of a contractor acting in accordance with 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 of which the Supplier is, or becomes, aware; and
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of placing cover representing any of the insurance to which it is a Party.

10.4.3 The Supplier will not do or omit to do anything, which would vitiate any of the insurances.

10.5 Indemnity to principals

10.5.1 Where specifically outlined in this Call-Off Contract, the Supplier will ensure that the third-party public and products liability policy will contain an 'indemnity to principals' clause under which the Buyer will be compensated for both of the following claims against the Buyer:

- death or bodily injury; and
- third-party Property damage arising from connection with the Services and for which the Supplier is legally liable.

10.6 Cancelled, suspended, terminated or unrenewed policies

10.6.1 The Supplier will notify CCS and any Buyers as soon as possible if the Supplier becomes aware that any of the insurance policies have been, or are due to be, cancelled, suspended, terminated or not renewed.

10.7 Premium, excess and deductible payments

10.7.1 Where any insurance requires payment of a premium, the Supplier will:

- be liable for the premium; and
- pay such premium promptly.

10.7.2 Where any insurance is subject to an excess or deductible below the Supplier will be liable for it. The Supplier will not be entitled to recover any sum paid for insurance excess or any deductible from CCS or the Buyer.

11. Confidentiality

11.1 Except where disclosure is clearly permitted by this Call-Off Contract, neither Party will disclose the other Party's Confidential Information without the relevant Party's prior written consent.

11.2 Disclosure of Confidential Information is permitted where information:

- must be disclosed to comply with legal obligations placed on the Party making the disclosure
- belongs to the Party making the disclosure (who is not under any obligation of confidentiality) before its disclosure by the information owner
- was obtained from a third party who is not under any obligation of confidentiality, before receiving it from the disclosing Party
- is, or becomes, public knowledge, other than by breach of this clause or Call-Off Contract
- is independently developed without access to the other Party's Confidential Information
- is disclosed to obtain confidential legal professional advice.

11.3 The Buyer may disclose the Supplier's Confidential Information:

- to any central government body on the basis that the information may only be further disclosed to central government bodies;
- to the UK Parliament, Scottish Parliament or Welsh or Northern Ireland Assemblies, including their committees;
- if the Buyer (acting reasonably) deems disclosure necessary or appropriate while carrying out its public functions;
- on a confidential basis to exercise its rights or comply with its obligations under this Call-Off Contract; or
- On a confidential basis to a proposed transferee, assignee or novatee of, or successor in title to, the Buyer.

11.4 References to disclosure on a confidential basis will mean disclosure subject to a confidentiality agreement or arrangement containing the same terms as those placed on the Buyer under this clause.

11.5 The Supplier may only disclose the Buyer's Confidential Information to Supplier Staff who are directly involved in the provision of the Services and who need to know the information to provide the Services. The Supplier will ensure that its Supplier Staff will comply with these obligations.

11.6 Either Party may use techniques, ideas or knowledge gained during this Call-Off Contract unless the use of these things results in them disclosing the other Party's Confidential Information where such disclosure is not permitted by the Framework Agreement, or is an infringement of Intellectual Property Rights.

11.7 Information about orders placed by a Buyer (including pricing information and the terms of any Call-Off Contract) may be published by CCS and may be shared with other Buyers. Where Confidential Information is shared with other Buyers, CCS will notify the recipient of the information that its contents are confidential.

12. Conflict of Interest

12.1 The Supplier will take all appropriate steps to ensure that Supplier Staff are not in a position where there is or may be an actual conflict between the financial or personal interests of the Supplier Staff and another Supplier where both are providing the Services to the Buyer under any Call-Off Contract in accordance with the Framework Agreement.

12.2 Any breach of this clause will be deemed to be a Material Breach.

12.3 A conflict of interest may arise in situations including where a member of the Supplier Staff:

- is related to someone in another Supplier team who both form part of the same team performing the Services under the Framework Agreement
- has a business interest in another Supplier who is part of the same team performing the Services under the Framework Agreement

- has been provided with, or had access to, information which would give the Supplier or an affiliated company an unfair advantage in the Tender process.

12.4 Where the Supplier identifies a risk of a conflict or potential conflict, they will (before starting work under this Call-Off Contract, unless otherwise agreed with the Buyer) inform the Buyer of such conflicts of interest and how they plan to mitigate the risk. Details of such mitigation arrangements are to be sent to the Buyer as soon as possible. On receiving this notification, the Buyer will, at its sole discretion, notify the Supplier if the mitigation arrangements are acceptable or whether the risk or conflict remains a Material Breach.

13. Intellectual Property Rights

13.1 The Supplier will have no rights to use any of the Buyer's names, logos or trademarks without the Buyer's prior written approval.

14. Data Protection and Disclosure

14.1 The Supplier shall comply with any notification requirements under the DPA and both Parties will duly observe all their obligations under the DPA which arise in connection with the Framework Agreement or under this Call-Off Contract.

14.2 Where the Supplier is processing Buyer Data or Other Contracting Bodies' Personal Data, the Supplier shall ensure that it has in place appropriate technical and organisational measures to ensure the security of the Authority and Other Contracting Bodies' Personal Data (and to guard against unauthorised or unlawful processing or accidental loss, destruction of or damage to the Buyer Data and the Other Contracting Bodies' Personal Data.

14.3 The Supplier shall provide the Buyer and/or Other Contracting Body with such information as the Buyer and/or Other Contracting Body may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA including;

- to promptly notify the Buyer and/or Other Contracting Body of any breach of the security measures to be put in place pursuant to this Clause; and
- to ensure that it does not knowingly or negligently do or omit to do anything which places the Buyer and/or Other Contracting Body in breach of its obligations under the DPA and
- not to cause or permit to be processed, stored, accessed or otherwise transferred outside the European Economic Area any Buyer Data or Other Contracting Body Personal Data supplied to it by the Buyer or Other Contracting Body without approval.

15. Buyer Data

15.1 The Supplier will not remove any proprietary notices relating to the Buyer Data.

15.2 The Supplier will not store or use Buyer Data except where necessary to fulfill its obligations.

15.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested and in the format specified by the Buyer.

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

15.5 The Supplier will ensure that any system which holds any Buyer Data complies with the security requirements prescribed by the Buyer.

15.6 The Supplier will ensure that any system on which the Supplier holds any protectively marked Buyer Data will be accredited as specific to the Buyer and will comply with:

- the government security policy framework and information assurance policy;
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management and Accreditation of Information Systems; and
- the relevant government information assurance standard(s).

15.7 Where the duration of this Call-Off Contract exceeds one year, the Supplier will review the accreditation status at least once a year to assess whether material changes have occurred which could alter the original accreditation decision in relation to Buyer Data. If any changes have occurred then the Supplier will re-submit such system for accreditation.

15.8 If at any time 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 where such corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier or its representatives) comply with any remedial action proposed by the Buyer.

15.9 The Supplier will provide at the request of CCS or the Buyer, any information relating to the Supplier's compliance with its obligations under the Data Protection Act (to the extent arising under and/or in connection with the Framework Agreement and this Call-Off Contract). The Supplier will also ensure that it does not knowingly or negligently fail to do something that places CCS or any Buyer in breach of its obligations of the Data Protection Act. This is an absolute obligation and is not qualified by any other provision of this Call-Off Contract.

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

15.11 The provisions of this Clause 15 shall apply during the term of this Call-Off Contract and for such time as the Supplier holds the Buyer's Data.

16. Records and audit access

16.1 The Supplier will allow CCS (and CCS's external auditor) to access its information and conduct audits of the Services provided under this Call-Off Contract and the provision of Management Information (subject to reasonable and appropriate confidentiality undertakings).

17. Freedom of Information (FOI) requests

17.1 The Supplier will transfer any Request for Information to the Buyer within 2 UK working days of receipt.

17.2 The Supplier will provide all necessary help reasonably requested by the Buyer to enable the Buyer to respond to the Request for Information within the time for compliance set out in section 10 of the Freedom of Information Act or Regulation 5 of the Environmental Information Regulations.

17.3 To the extent it is permissible and reasonably practical for it to do so, CCS will make reasonable efforts to notify the Supplier when it receives a relevant FOIA or EIR request so that the Supplier may make appropriate representations.

18. Standards and quality

18.1 The Supplier will comply with any standards in this Call-Off Contract and Section 4 (How Services will be delivered) of the Framework Agreement.

19. Security

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

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

19.3 Any costs arising from the actions of the Buyer or Supplier taken in compliance with the provisions of the above clause, will be dealt with by the Buyer and the Supplier as follows:

- by the Supplier, where the Malicious Software originates from the Supplier software or the Buyer Data while the Buyer Data was under the control of the Supplier, unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier.
- by the Buyer if the Malicious Software originates from the Buyer software or the Buyer Data, while the Buyer Data was under the control of the Buyer.

19.4 The Supplier will immediately notify CCS of any breach of security in relation to CCS's Confidential Information (and the Buyer in relation to any breach regarding Buyer Confidential Information). The Supplier will recover such CCS and Buyer Confidential Information however it may be recorded.

19.5 Any system development by the Supplier must also comply with the government's '10 Steps to Cyber Security' guidance, available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

20. Guarantee

20.1 Where the Buyer has specified in the Order Form that this Call-Off Contract shall be conditional upon receipt of a Guarantee from the guarantor, the Supplier shall deliver to the Buyer a completed Guarantee in the form attached, on or prior to the Commencement Date; and deliver to the Buyer a certified copy of the passed resolution and/or board minutes of its guarantor approving the execution of the Guarantee.

21. Incorporation of terms

21.1 Upon the execution of an Order, the terms and conditions agreed in the Order Form will be incorporated into this Call-Off Contract.

22. Managing disputes

22.1 When either Party notifies the other of a dispute, both Parties will attempt in good faith to negotiate a settlement as soon as possible.

22.2 Nothing in this procedure will prevents a Party from seeking any interim order restraining the other Party from doing any act or compelling the other Party to do any act.

22.3 If the dispute cannot be resolved, either Party will be entitled to refer it to mediation in accordance with the procedures below, unless:

- the Buyer considers that the dispute is not suitable for resolution by mediation,
- the Supplier does not agree to mediation.

22.4 The procedure for mediation is as follows:

- A neutral adviser or mediator will be chosen by agreement between the Parties. If the Parties cannot agree on a mediator within 10 UK working days after a request by one Party to the other, either Party will as soon as possible, apply to the mediation provider or to the Centre for Effective Dispute Resolution (CEDR) to appoint a mediator. This application to CEDR must take place within 12 UK working days from the date of the proposal to appoint

a mediator, or within 3 UK working days of notice from the mediator to either Party that they are unable or unwilling to act.

- The Parties will meet with the mediator within 10 UK working days of the mediator's appointment to agree a programme for the exchange of all relevant information and the structure for negotiations to be held. The Parties may at any stage seek help from the mediation provider specified in this clause to provide guidance on a suitable procedure.
- Unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings.
- If the Parties reach agreement on the resolution of the dispute, the agreement will be reduced to writing and will be binding on the Parties once it is signed by their duly authorised representatives.
- Failing agreement, either Party may invite the mediator to provide a non-binding but informative opinion in writing. Such an opinion will be provided without prejudice and will not be used in evidence in any proceedings relating to this Call-Off Contract without the prior written consent of both Parties.
- If the Parties fail to reach agreement in the structured negotiations within 60 UK working days of the mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the courts.

22.5 Either Party may request by written notice that the dispute is referred to expert determination if the dispute relates to:

- any technical aspect of the delivery of the digital services;
- the underlying technology; or
- otherwise is of a financial or technical nature.

22.6 An expert will be appointed by written agreement between the Parties, but if there is a failure to agree within 10 UK working days, or if the person appointed is unable or unwilling to act, the expert will be appointed on the instructions of the President of the British Computer Society (or any other association that has replaced the British Computer Society).

22.7 The expert will act on the following basis:

- they will act as an expert and not as an arbitrator and will act fairly and impartially;
- the expert's determination will (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;
- the expert will decide the procedure to be followed in the determination and will be requested to make their determination within 30 UK working days of their appointment or as soon as reasonably practicable and the Parties will help and provide the documentation that the expert needs for the determination;

- any amount payable by one Party to another as a result of the expert's determination will be due and payable within 20 UK working days of the expert's determination being notified to the Parties
- the process will be conducted in private and will be confidential;
- the expert will determine how and by whom the costs of the determination, including their fees and expenses, are to be paid.

22.8 Without prejudice to any other rights of the Buyer under this Call-Off Contract, the obligations of the Parties under this Call-Off Contract will not be suspended, ceased or delayed by the reference of a dispute submitted to mediation or expert determination and the Supplier and the Supplier Staff will comply fully with the Requirements of this Call-Off Contract at all times.

23. Termination

23.1 The Buyer will have the right to terminate this Call-Off Contract at any time by giving the notice to the Supplier specified in Part A, the Order Form. The Supplier's obligation to provide the Services will end on the date set out in the Buyer's notice.

23.2 The Parties acknowledge and agree that:

- the Buyer's right to terminate under this clause is reasonable in view of the subject matter of this Call-Off Contract and the nature of the Service being provided.
- the Call-Off Contract Charges paid during the notice period given by the Buyer in accordance with this clause are a reasonable form of compensation and are deemed to fully cover any avoidable costs or losses incurred by the Supplier which may arise either directly or indirectly as a result of the Buyer exercising the right to terminate under this clause without cause.
- Subject to clause 31 (Liability), if the Buyer terminates this Call-Off Contract without cause, they 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 such Loss. If the Supplier holds insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of such Loss, with supporting evidence of unavoidable Losses incurred by the Supplier as a result of termination.
- Either Party will have the right to terminate this Call-Off Contract where clause 29.2 applies.

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

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

23.4 Either Party may terminate this Call-Off Contract at any time with immediate effect by written notice (of not more than 30 UK working days) if the other Party commits a

Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due under this Call-Off Contract) and, if such breach is remediable, fails to remedy that breach within a period of 15 UK working days of being notified in writing to do so.

23.5 If an Insolvency Event of either Party occurs, or the other Party ceases or threatens to cease to carry on the whole or any material part of its business, the other Party is entitled to terminate this Call-Off Contract with immediate effect.

23.5 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier shall notify the Buyer in writing of such failure to pay and allow the Buyer five (5) calendar days to settle the undisputed invoice. If the Buyer fails to pay such undisputed sums within the allotted additional 5 calendar days, the Supplier may terminate this Call-Off Contract subject to giving the length of notice specified in the Order Form (Termination)

24. Consequences of termination and expiry

24.1 Where the Buyer has the right to terminate this Call-Off Contract it may elect to suspend this Call-Off Contract and its performance.

24.2 If the Buyer contracts with another Supplier for the Deliverables under this Call-Off Contract, the Supplier will comply with clause 28.

24.3 The rights and obligations of the Parties in respect of this Call-Off Contract will automatically terminate upon the expiry or termination of this Call-Off Contract, except those rights and obligations set out in clause 24.7.

24.4 At the end of the Call-Off Contract period (howsoever arising), the Supplier must:

- promptly return to the Buyer:
  - all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under this Call-Off Contract;
  - any materials created by the Supplier under this Call-Off Contract where the IPRs are owned by the Buyer;
  - cease to use the Buyer Data and, at the direction of the Buyer, provide the Buyer and the replacement Supplier with a complete and uncorrupted version of the Buyer Data in electronic form in the formats and on media agreed with the Buyer and the replacement Supplier;
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 months after the date of expiry or termination, and provide written confirmation to the Buyer that the data has been securely destroyed, except where the retention of Buyer Data is required by Law;
- work with the Buyer on any work in progress and ensure an orderly transition of the Services to the replacement supplier;
- return any sums prepaid for Services which have not been delivered to the Buyer by the date of expiry or termination;

- provide all information requested by the Buyer on the provision of the Services so that:
  - the Buyer is able to understand how the Services have been provided; and
  - the Buyer and the replacement supplier can conduct due diligence.

24.5 Each Party will return all of the other Party's Confidential Information. Each Party will confirm that it does not retain the other Party's Confidential Information except where the information must be retained by the Party as a legal requirement or where this Call-Off Contract states otherwise.

24.6 All licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Services will be terminated at the end of the Call-Off Contract period (howsoever arising) without the need for the Buyer to serve notice except where this Call-Off Contract states otherwise.

24.7 Termination or expiry of this Call-Off Contract will not affect:

- any rights, remedies or obligations accrued under this Call-Off Contract prior to termination or expiration;
- the right of either Party to recover any amount outstanding at the time of such termination or expiry;
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses:
  - 8 - Payment Terms and VAT
  - 9 - Recovery of Sums Due and Right of Set-Off
  - 10 - Insurance
  - 11 - Confidentiality
  - 12 - Conflict of Interest
  - 13 - Intellectual Property Rights
  - 15 - Buyer Data
  - 24 - Consequences of Expiry or Termination
  - 31 - Liability
  - 32 - Waiver and cumulative remedies
- any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is to be performed or observed notwithstanding termination or expiry will survive the termination or expiry of this Call-Off Contract.

25. Supplier's status

25.1 The Supplier is an independent Contractor and no contract of employment or partnership is created between the Supplier and the Buyer. Neither Party is authorised to act in the name of, or on behalf of, the other Party.

26. Notices

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

26.2 The following table sets out the method by which notices may be served under this Call-Off Contract and the respective deemed time and proof of Service:

Delivery type	Deemed delivery time	Proof of Service
Email	9am on the first Working Day after sending	Dispatched in a pdf form to the correct email address without any error message

26.3 The address and email address of each Party will be the address and email address in the Order Form.

27. Exit plan

27.1 The Supplier has provided details of their exit plan within the service description specified in the Order Formand the Buyer and Supplier will follow these arrangements as per Supplier Terms.

28. Handover to replacement supplier

28.1 Within 10 UK Working Days of the expiry or termination of this Call-Off Contract , the Supplier will make available to the Buyer:

- any data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control.
- any sums prepaid to the Supplier in respect of Ordered Deliverables not provided by the date of expiry or termination of this Call-Off Contract.

28.2 When requested, the Supplier will (at its own expense where the Call-Off Contract has been terminated before end of term due to Supplier cause) help the Buyer to migrate the Services to a replacement Supplier in line with the exit plan (clause 27) to ensure continuity of the Services.

29. Force Majeure

29.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event. Each Party will use all reasonable endeavours to continue to perform its obligations under this Call-Off Contract for the length of a Force Majeure event.

29.2 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 15 consecutive calendar days, the other Party may terminate this Call-Off Contract with immediate effect by notice in writing.

30. Entire agreement

30.1 This Call-Off Contract constitutes the entire agreement between the Parties relating to the matters dealt within it. It supersedes any previous agreement between the Parties relating to such matters.

30.2 Each Party agrees that in entering into this Call-Off Contract it does not rely on, and will have no remedy relating to, any agreement or representation (whether negligently or innocently made) other than as expressly described in this Call-Off Contract.

30.3 Nothing in this clause will exclude any liability for (or remedy relating to) fraudulent misrepresentation or fraud.

30.4 Each of the Parties agrees that in entering into this Call-Off Contract it does not rely on, and will have no remedy relating to, any agreement, statement, representation, warranty, understanding or undertaking (whether negligently or innocently made) other than as described in this Call-Off Contract.

31. Liability

31.1 Neither Party excludes or limits its liability for:

- death or personal injury;
- bribery or fraud by it or its employees;
- breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or sections 2 or 11B of the Supply of Goods and Services Act 1982; or
- any liability to the extent it cannot be excluded or limited by Law.

31.2 Subject to Clauses 31.1 and 31.10 and any lower limits specified in the Order Form, and notwithstanding Clause 31.4, each Party's total aggregate liability relating to all Losses due to a Default in connection with this Call-Off Contract::

- resulting in direct loss or damage to physical Property (including any technical infrastructure, assets or Equipment) of the other Party, will be limited to the sum of £1,000,000 in each Call-Off Contract year in which the Default occurs
- subject to the first bullet point in this clause 31.2 which occur in the first 6 months,will be limited to the greater of the sum of £500,000 or a sum equal to 200% of the estimated Call-Off Contract Charges for the first six months
- subject to the first bullet point in this clause 31.2 which occur during the remainder of the Call-Off Contract period,will be limited to the greater of the sum of £500,000 or an amount equal to 125% of the Call-Off Contract Charges paid, due or which would have been payable under this Call-Off Contract in the 6 months immediately preceding the event giving rise to the liability
- subject to the first bullet point in this clause 31.2 which occur after the end of the Call-Off Contract period, will be limited to the greater of the sum of £500,000 or an amount equal to 125% of the Call-Off Contract Charges paid, due or which would have been payable under this Call-Off Contract in the 6 months immediately before the end of the Call-Off Contract period.

31.3 Subject to clause 31.1, 31.4, in no event will either Party be liable to the other for any:

- loss of profits;
- loss of business;

- loss of revenue;
- loss of or damage to goodwill;
- loss of savings (whether anticipated or otherwise); or
- any indirect, special or consequential loss or damage.

31.4 Subject to Clause 31.2 the Supplier will be liable for the following types of loss which will be regarded as direct and will be recoverable by the Buyer:

- the additional operational or administrative costs and expenses arising from any Supplier Default; and
- any wasted expenditure or charges rendered unnecessary and/or incurred by the Buyer arising from the Supplier's Default; and
  any losses, costs, damages, expenses or other liabilities suffered or incurred by the Buyer which arise out of or in connection with the loss of, corruption or damage to or failure to deliver Buyer Data by the Supplier; and
- any regulatory losses, fines, expenses or other losses arising from a breach by the Supplier of any Law.

31.5 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Buyer Data or the Buyer Personal Data or any copy of such Buyer Data, caused by the Supplier's default under or in connection with a Call-Off Contract shall be subject to the financial limits set out in the Order Form.

31.6 No enquiry, inspection, approval, sanction, comment, consent, or decision at any time made or given by, or on behalf of, the Buyer to any document or information provided by the Supplier in its provision of the Services, and no failure of the Buyer to discern any defect in, or omission from, any such document or information will exclude or limit the obligation of the Supplier to carry out all the obligations of a professional Supplier employed in a client and Buyer relationship.

31.7 Unless otherwise expressly provided, the obligations of the Buyer under this Call-Off Contract are obligations of the Buyer in its capacity as a Contracting counterparty and nothing in this Call-Off Contract will be an obligation on, or in any other way constrain the Buyer in any other capacity, nor will the exercise by the Buyer of its duties and powers in any other capacity lead to any liability under this Call-Off Contract on the part of the Buyer to the Supplier.

31.8 Any liabilities which are unlimited will not be taken into account for the purposes of establishing whether any limits relating to direct loss or damage to physical Property within this clause have been reached.

31.9 The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Buyer or by breach by the Buyer of its Call-Off Contract obligations.

31.10 The Supplier's liability to pay any Management Charges which are payable to the Authority shall not be limited.

32. Waiver and cumulative remedies

32.1 The rights and remedies provided by this agreement may be waived only in writing by the Buyer or the Supplier representatives in a way that expressly states that a waiver is intended, and such waiver will only be operative regarding the specific circumstances referred to.

32.2 Unless a right or remedy of the Buyer is expressed to be exclusive, the exercise of it by the Buyer is without prejudice to the Buyer's other rights and remedies. Any failure to exercise, or any delay in exercising, a right or remedy by either Party will not constitute a waiver of that right or remedy, or of any other rights or remedies.

33. Fraud

33.1 The Supplier will notify the Buyer if it suspects that any fraud has occurred, or is likely to occur. The exception to this is if while complying with this, it would cause the Supplier or its employees to commit an offence.

33.2 If the Supplier commits any fraud relating to a Framework Agreement, this Call-Off Contract or any other Contract with the government:

- the Buyer may terminate the Call-Off Contract
- CCS may terminate the Framework Agreement
- CCS and/or the Buyer may recover in full from the Supplier whether under Clause 33.3 below or by any other remedy available in law.

33.3 The Supplier will, on demand, compensate CCS and/or the Buyer, in full, for any loss sustained by CCS and/or the Buyer at any time (whether such loss is incurred before or after the making of a demand following the indemnity hereunder) in consequence of any breach of this clause.

34. Prevention of bribery and corruption

34.1 The Supplier will not commit any Prohibited Act.

34.2 The Buyer and CCS will be entitled to recover in full from the Supplier and the Supplier will, on demand, compensate CCS and/or the Buyer in full from and against:

- the amount of value of any such gift, consideration or commission; and
- any other loss sustained by CCS and/or the Buyer in consequence of any breach of this clause.

35. Legislative change

35.1 The Supplier will neither be relieved of its obligations under this Call-Off Contract nor be entitled to increase the Call-Off Contract prices as the result of a general change in Law or a Specific Change in Law without prior written approval from the Buyer.

36. Publicity, branding, media and official enquiries

36.1 The Supplier will take all reasonable steps to not do anything which may damage the public reputation of the Buyer. The Buyer may terminate this Call-Off Contract for Material Breach where the Supplier, by any act or omission, causes material adverse publicity relating to or affecting the Buyer or the Call-Off Contract. This is true whether or not the act or omission in question was done in connection with the performance by the Supplier of its obligations hereunder.

37. Non Discrimination

37.1 The Supplier will notify CCS and relevant Buyers immediately of any legal proceedings issued against it by any Supplier Staff on the grounds of discrimination.

38. Premises

38.1 Where either Party uses the other Party's premises, such Party is liable for all Loss or damage it causes to the premises. Such Party is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

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

38.3 The Supplier will vacate the Buyer's premises upon termination or expiry of the Call-Off Contract.

38.4 This clause does not create an tenancy or exclusive right of occupation.

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

- ensure 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;
- comply with any instructions from the Buyer on any necessary associated safety measures ; and
- notify the Buyer immediately in the event of any incident occurring on the premises where that incident causes any personal injury or damage to Property which could give rise to personal injury.

38.6 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.

38.7 All Equipment brought onto the Buyer's premises will be at the Supplier's risk. Upon termination or expiry of the Call-Off Contract, the Supplier will remove such Equipment.

39. Equipment

39.1 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.

39.2 Upon termination or expiry of the Call-Off Contract, the Supplier will remove the Equipment, and any other materials, leaving the premises in a safe and clean condition.

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

40.1 A person who is not party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Call-Off Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

41. Law and jurisdiction

41.1 This Call-Off Contract will be governed by the Laws of England and Wales. Each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

42. Environmental requirements

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

42.2 The Supplier must support Buyers in their efforts to work in an environmentally-friendly way, eg by helping them engage in practices like recycling or lowering their carbon footprint.

43. Defined Terms

In this Call-Off Contract, the following expressions and defined terms have the following interpreted meaning:

'Additional Services'	The services in addition to the G-Cloud Services which are within the scope of the Framework Agreement which the Buyer may request from time to time.
'Application'	The response submitted by the Supplier to the Invitation to Tender (ITT).
'Assurance'	The verification process undertaken by CCS as described in this Framework Agreement.
'Background IPRs'	For each Party: ● IPRs owned by that Party before the date of this Call-Out Contract, including IPRs contained in any of the Party's know-how, documentation, processes and procedures, ● IPRs created by the Party independently of this Call-Out Contract, and/or ● For the Buyer, Crown Copyright which is not available to the Supplier otherwise than under this Call-Out Contract, but excluding IPRs owned by that Party subsisting in Buyer software or Supplier software.
'Buyer'	A UK public sector body, or Contracting Body, as described in

	the OJEU Contract Notice, that can execute a competition and a Call-Off Contract within this Framework Agreement and is identified in the Call-Off Order Form.
'Buyer's Confidential Information'	All Buyer Data and any information that relates to the business, affairs, developments, trade secrets, know-how, personnel, and Suppliers of the Buyer, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above Any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
'Buyer Data'	Data that is owned or managed by the Buyers.
'Buyer Software'	Software owned by or licensed to the Buyer (other than under or pursuant to this Agreement), which is or will be used by the Supplier for the purposes of providing the Services.
'Call-Off Contract'	The legally binding agreement (entered into following the provisions of this Framework Agreement) for the provision of Services made between a Buyer and the Supplier. This may include the Order Form detailing service requirements, term of Call-Off Order, start date and pricing.
'Charges'	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract.
'PSN Code of Practice'	Those obligations and requirements for PSN Service Providers wanting to participate in the PSN together with all documents annexed to it and referenced within it, as set out in the code template.
'Collaboration Agreement'	An agreement between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives an efficient end-to-end G-Cloud Services.
'Commencement Date'	For the purposes of the Framework Agreement, commencement date shall be as outlined in Section 1 - The Appointment within this Framework Agreement. For the purposes of the Call-Off Contract, commencement date shall be as set in the Order Form.
'Commercially Sensitive Information'	Information, which CCS has been notified about, (before the start date of the Framework Agreement) or the Buyer (before the Call-Off Contract start date) with full details of why the Information is deemed to be commercially sensitive.
'Comparable Supply'	The supply of services to another Buyer of the Supplier that are the same or similar to any of the Services

'Confidential Information'	CCS's Confidential Information or the Supplier's Confidential Information, which may include (but is not limited to): ● any information that relates to the 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 ● any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential'
'Contracting Bodies'	The Buyer and any other person as listed in the OJEU Notice or Regulation 2 of the Public Contracts Regulations 2015, as amended from time to time, including CCS
'Control'	Control as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly
'Crown'	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf
'Data Protection Legislation or DPA'	The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable legally binding guidance and codes of practice issued by the Information Commissioner.
'Data Subject'	Shall have the same meaning as set out in the Data Protection Act 1998, as amended from time to time.
'Default'	● any breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● any other default, act, omission, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff in connection with or in relation to this Framework Agreement or this Call-Off Contract Unless otherwise specified in this Call-Off Contract the Supplier

	is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
'Deliverable'	Those G-Cloud Services which the Buyer contracts the Supplier to provide under the Call Off Contract.
'Digital Marketplace'	The government marketplace where Services will be made available to Buyers to enable them to be bought (https://www.digitalmarketplace.service.gov.uk/)
'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 the Call-Off Contract.
'Direct Award Criteria'	The award criteria to be applied for the award of Call-Off Contracts for G-Cloud Services set out in Section 3 'Buying Process'.
'Direct Ordering Procedure'	The ordering procedure set out in Framework Agreement.
'Effective Date'	The date on which the Call-Off Contract is signed and as set out in the Order Form.
'FoIA'	The Freedom of Information Act 2000 and any subordinate legislation made under the Act occasionally together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation.
'Framework Agreement'	The contractually-binding framework agreement between the Crown Commercial Service and the Supplier, reference number: RM1557viii, referred to in the Order Form.
'Framework Suppliers'	The suppliers (including the Supplier) appointed under this G-Cloud 8 Framework Agreement.
'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 Framework Agreement or defrauding or attempting to defraud or conspiring to defraud the Crown.
'G-Cloud Services'	The cloud services described in Framework Section 2 (G-Cloud Services) as defined by the Service Definition, the Supplier Terms and any related tender documentation, which the Supplier shall make available to the Authority and Other Contracting Bodies and those services which are deliverable by

	the Supplier under the Collaboration Agreement.
'Good Industry Practice'	Standards and procedures conforming to the Law and the application of skill, care and foresight which would be expected from a person or body who has previously been engaged in a similar type of undertaking under similar circumstances. The person or body must adhere to the technology code of practice (https://www.gov.uk/service-manual/technology/code-of-practice.html) and the government service design manual (https://www.gov.uk/service-manual).
'Group'	A company plus any subsidiary or Holding Company. 'Holding company' and 'Subsidiary' are defined in section 1159 of the Companies Act 2006.
'Group of Economic Operator'	A partnership or consortium not (yet) operating through a separate legal entity.
'Guarantee'	The deed of guarantee described in the Order Form (Parent Company Guarantee).
'Guidance'	Any current UK Government Guidance on the Public Contracts Regulations. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance shall take precedence.
'Holding Company'	As described in section 1159 and Schedule 6 of the Companies Act 2006.
'Information'	As described under section 84 of the Freedom of Information Act 2000, as amended from time to time.
'Insolvency Event'	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium.
'Intellectual Property Rights' or 'IPR'	means: a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, service marks, logos, database rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, design rights (whether registerable or otherwise), know-how, trade secrets and moral rights and other similar rights or obligations whether registerable or not; b) applications for registration, and the right to apply for

	registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights whether registerable or not having equivalent or similar effect in any country or jurisdiction (including but not limited to the United Kingdom) and the right to sue for passing off.
'Invitation to Tender or ITT'	The invitation to tender for this Framework.
'Law'	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of Law, or directives or requirements of any Regulatory Body.
'Loss'	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
'Lot'	A subdivision of the Services which are the subject of this procurement as described in the OJEU Contract Notice.
Management Charge"	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.5% 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 termination of any Call-Off Contract.
'Management Information'	The management information (MI) specified in section 6 (What you report to CCS) of the Framework Agreement.
'Management Information (MI) Failure'	If any of the below instances occur, CCS may treat this as an 'MI Failure': ● there are omissions or errors in the Supplier's submission ● the Supplier uses the wrong template ● the Supplier's report is late ● the Supplier fails to submit a report
'Material Breach (Framework Agreement)'	A breach by the Supplier of the following Clauses in this Framework Agreement: ● Subcontracting ● Non-Discrimination ● Conflicts of Interest and Ethical Walls ● Warranties and Representations ● Provision of Management Information ● Management Charge

	• Prevention of Bribery and Corruption • Safeguarding against Fraud • Data Protection and Disclosure • Intellectual Property Rights and Indemnity • Confidentiality • Official Secrets Act • Audit
'Material Breach (Call-Off Contract)'	A single serious breach of or persistent failure to perform as required in the Call-Off Contract.
'OJEU Contract Notice'	The advertisement for this procurement issued in the Official Journal of the European Union.
'Order Form'	An order set out in the Call-Off Contract for G-Cloud Services placed by a Buyer with the Supplier.
'Other Contracting Bodies'	All Contracting Bodies, or Buyers, except CCS.
'Parent Company'	Any company which is the ultimate Holding Company of the Supplier.
'Party'	• for the purposes of the Framework Agreement, CCS or the Supplier • for the purposes of the Call-Off Contract, the Supplier or the Buyer and 'Parties' will be interpreted accordingly.
'Personal Data'	As described in the Data Protection Act 1998 (http://www.legislation.gov.uk/ukpga/1998/29/contents)
'Prohibited Act'	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: O under the Bribery Act 2010 O under legislation creating offences concerning Fraud O at common Law concerning Fraud O committing or attempting or conspiring to commit Fraud
'PSN'	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
'Regulations'	The Public Contracts Regulations 2015 (at http://www.legislation.gov.uk/uksi/2015/102/contents/made) and the Public Contracts (Scotland) Regulations 2012 (at http://www.legislation.gov.uk/ssi/2012/88/made).
'Regulatory 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 Framework Agreement.
'Reporting Date'	The seventh day of each month following the month to which the relevant MI relates. A different date can be chosen if agreed between the Parties.
'Request for Information'	A request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations.
'Self Audit Certificate'	The certificate in the form as set out in Framework Schedule 1 - Self Audit Certificate, to be provided to CCS by the Supplier.
'Services'	Means G-Cloud Services and any/or Additional Services.
'Service Definition'	The definition of the Supplier's G-Cloud Services provided as part of their Tender that includes, but is not limited to, those items listed in Section 2 (G-Cloud Services) of this Framework Agreement.
'Service Description'	The description of the Supplier service offering as published on the Digital Marketplace.
'Standstill Period'	The term Standstill Period is set out in Regulation 87 (2). In summary, it is the 10 calendar days after CCS (in this instance by electronic means) sends its decision to conclude the Framework Agreement tendered via the Official Journal of the European Union, during which CCS must not conclude the Framework Agreement with the successful Supplier(s). Unsuccessful Applicants can raise any questions with CCS that relate to the decision to award before the Framework Agreement is concluded. CCS cannot advise unsuccessful Applicants on the steps they should take. Applicants should always seek independent legal advice, where appropriate.
'Specific Change in Law'	A change in the Law that relates specifically to the business of CCS and which would not affect a Comparable Supply.
'Subcontractor'	Each of the Supplier's Subcontractors or any person engaged by the Supplier in connection with the provision of the digital services as may be permitted by this Framework Agreement.
'Supplier'	A Supplier of G-Cloud Services who can bid for Call-Off Contracts as outlined in the Contract Notice within the Official Journal of the European Union (OJEU Contract Notice).
'Supplier Background IPRs'	Background IPRs of the Supplier.
'Supplier Insolvency Event'	Means the Supplier is unable to pay debts in Section 268 of Insolvency Act 1986.
'Supplier Staff'	All persons employed by the Supplier including the Supplier's agents and consultants used in the performance of its obligations under this Framework Agreement or any Call-Off

	Contracts.
'Supplier Terms'	means the terms and conditions pertaining to the G-Cloud Services and as set out in the Terms and Conditions document supplied as part of the Supplier's Tender.
'Tender'	The response submitted by the Supplier to the Invitation to Tender.
'Working Day'	Any day other than a Saturday, Sunday or public holiday in England and Wales , from 9am to 5pm unless otherwise agreed with the Buyer and the Supplier in the Call-Off Contract.

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.

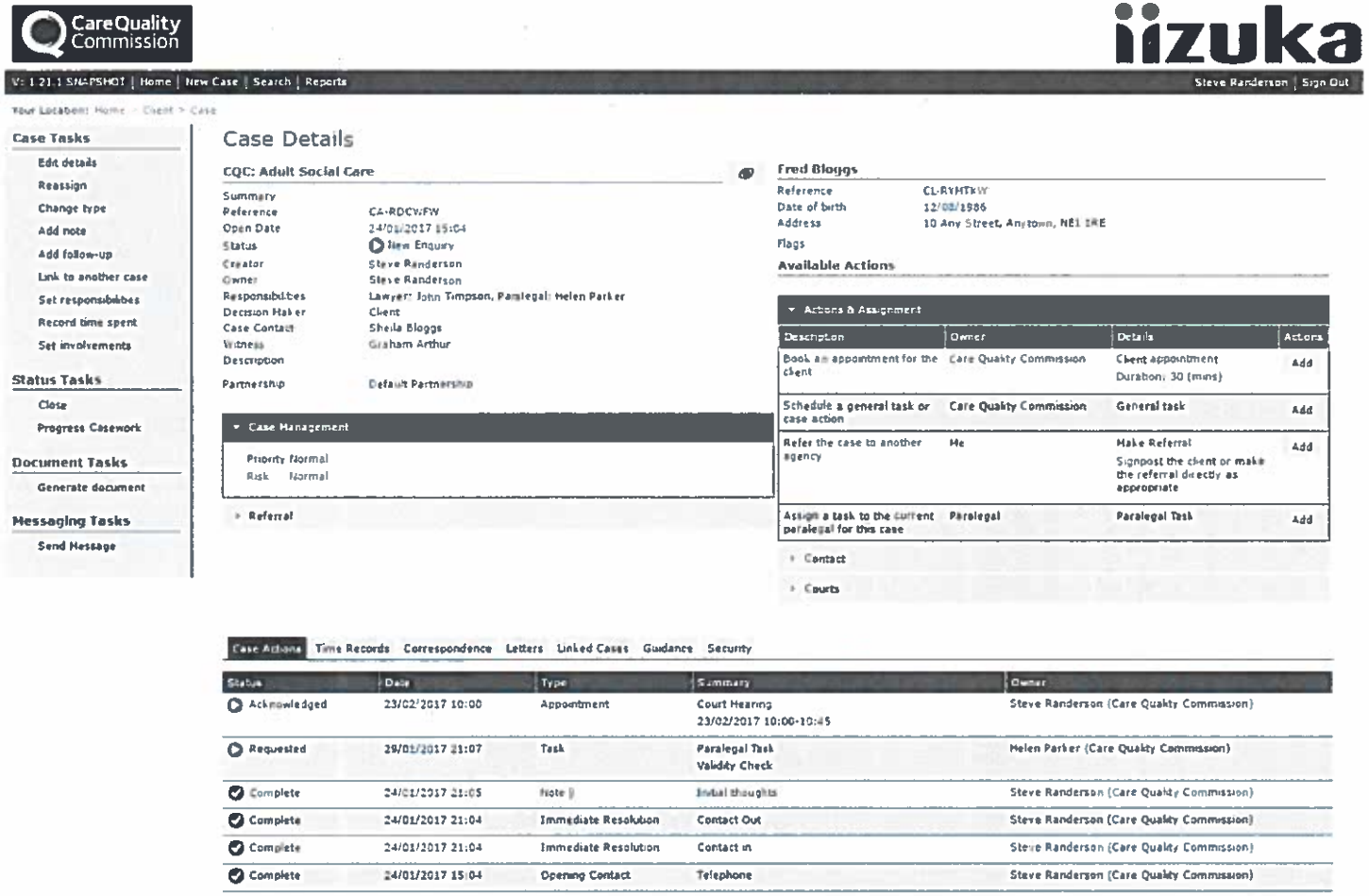
IIZUKA has a proven track record of delivering reliable, mission critical and highly secure systems to organisations such as the Foreign & Commonwealth Office, the Pensions Ombudsman and numerous local authorities, advice agencies, emergency services, housing associations, industry bodies and more.

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.

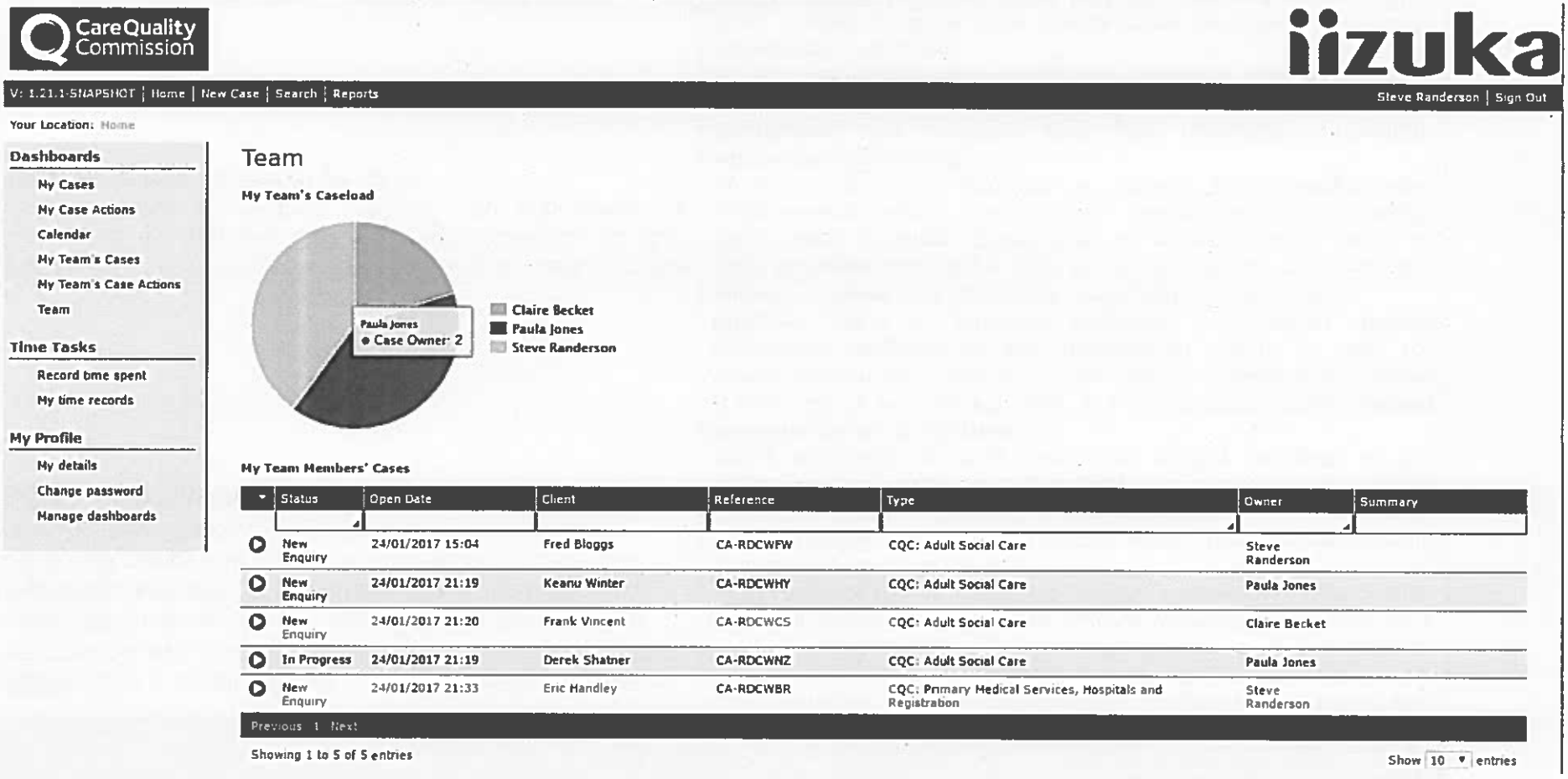
Screenshot 1 – Case Screen

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.



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.



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

	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.

[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)	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.
[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	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.
[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)	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.
[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)	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

	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

	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.

[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	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.
[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	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.
As a Manager, I want to be able to review the completed and outstanding judges orders	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.
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.	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

	make updates as required.
[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)	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.
[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).	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.
Tasks, Templates and Prompts	
[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 a). I can readily see from the document list which sector it belongs to b). I can manage my case efficiently	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.
[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)	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,

	users can make amendments to the document before it is finalised, published and made a permanent part of the case record.
[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)	Case Manage 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.
[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)	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.
[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)	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.
Management Information Reporting	
[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.	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.
[SCM-26] As a Legal Manager (Advisor) I need the ability to report on the present workload of internal and external Legal	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.

Advisors so that I can predict the future capacity needs of the 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)	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.
[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.	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.
[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.	Case Manager allows a wide range of report types to be generated including performance reports for specific teams or groups of users.
[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	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

complaints; Region; Directorate and Complaints Status) (MUST)	ensure that only relevant cases are included in each 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).	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,
[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 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	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. Capacity management is achieved through dashboards and managemtn information reports that show the current and past allocation of work across individuals, teams and organisations.
Manage cases- Search, Archive & Retrieve cases	
[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 (QRAM- QUALITY REVIEW ASSURANCE MANAGEMENT).	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 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.
[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)	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. Cases are also linked to other records, such as records of external organisations, providers, laywers 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 laywer.
[**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)	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.
[SCM-68] As a User, I want to have the ability to archive cases, so that I can comply with legislation (MUST)	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.

	Case Manager also supports rule based anonymisation or deletion of cases, so that data protection legislation 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	Case Manager has a Time Recording module that allows users

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	to record time against cases, against individual actions within cases or generally, where time is spent not working on specific 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.
[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)	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.
[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	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.
[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	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 general resources.
[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)	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. 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.
[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)	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. This allows the system to generate clear outputs of what time was spent, by whom and doing what.
Digital Division of Labour	
[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	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.
[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	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

the sector (MUST)	also allows cases to be linked to records of people or organisations, so that all cases involving them can easily be identified.
Quality control feedback	
[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	Case Manager allows actions and reports to be scheduled in advance, according to workflows and configured deadlines.
[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 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	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. 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.
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?	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. Further functions allow users to record time spent on different categories of non-casework activities, and so give a fuller

	account of their time

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	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.

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.	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	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

network and provide mechanisms for reporting on and controlling that load.		Manger 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 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
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.	N/A	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. 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
Integration		
Integration - System must support authentication using CQC's existing active directory as part of its existing infrastructure managed service (Open Service) using ADFS.	Full	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.
Interface requirements - Where relevant to its function, the system shall be capable of interfacing with CQC internal and external data sources, such as	Full	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

Siebel CRM, OBIEE, Oracle 11g, MySql, PostgreSQL and SQLServer 2008 and above, making use of CQC's Mulesoft Anypoint platform for transactional integration. As stated in the Architecture Principles, a service oriented approach should be used, where practical and possible.		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
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	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.

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.	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 channels.
	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.	Full	Case Manager is a highly configurable system that can be managed by authorised business users. IIZUKA will provided 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. 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. 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. 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.
Release Management - System to be subject to formal processes for release management, in association with customer with regard to testing.	Full	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 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.
Segregation of environments - Responsibilities related to program coding, application testing and approval, program transfer between environments are segregated	Full	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.
	Usability	
Language support - The application must support UK English.	Full	The application is built to support UK English
Desktop support - All system configuration settings are remotely accessible to the system administrator through application	Full	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

screens or setup programs (i.e. no hard coded system variables exist and include system, user, roles, company and other configuration screens).		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.
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	Full	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 Case Manager also supports configurable views of information, allowing regularly accessed information to be combined into easy to access displays.
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	Full	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. Should the CQC upgrade to a 64 bit client then Case Manager is already fully compatible with this. As a hosted managed service no systems administration or installation guides are required. 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.

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.	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 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.

<table>
<tr><th>Support</th><th></th><th></th></tr>
<tr><td>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.</td><td>Full</td><td>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. 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:
<table>
<tr><th>Severity level</th><th>Definition</th><th>Response time</th><th>Resolution target (SSHs)</th><th>Examples</th></tr>
<tr><td>1</td><td>Failure of business critical function</td><td>30 minutes</td><td>4</td><td>Main business use interruption (e.g.unable to process cases or to run report at month end). Apparent loss of business critical data.</td></tr>
<tr><td>2</td><td>Defect in high usage function</td><td>30 minutes</td><td>16</td><td>Functional error preventing use of specific screen within a case (e.g. unable to record notes).</td></tr>
<tr><td>3</td><td>Defect in low usage function</td><td>30 minutes</td><td>40</td><td>Search returning incorrect results.
Failure to send reminder emails.</td></tr>
<tr><td>4</td><td>Non-functional defect</td><td>30 minutes</td><td>By agreement</td><td>Inconsistent sorting, Unintended process outcome. Typographical or layout error.</td></tr>
</table>
The response times for customer support queries is 30 minutes.</td></tr>
</table>

		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 downtime (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 not 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.

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

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.

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

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

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

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.		within the update. Support for old versions is not applicable to a hosted managed service.
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.	Full	All credentials used by the system are stored only in encrypted form and are deciphered using un-shared keys.
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.	Full	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
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.	Full	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.
Account lock out - The number of failed login attempts before system lockout is 5 attempts or less and this	Full	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

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.	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		
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.	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
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.	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		
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,	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

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

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.	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	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

data retention policy?		specifically marked for retention, however this will be reviewed with the CQC during the requirements analysis phase of the project.

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	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. 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.
4.2 Applications are independent of technology platforms	Full	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 Case Manager itself is written using industry best practice approaches, in platform

		independent languages and using open source elements wherever possible. The 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 PosgreSQL, but with MS SQL Server available as a further option. Integration and communication with other systems are achieved through best practice approaches using web services, typically with XML or JSON payloads
4.3 A Service Orientated Architecture must be used	Full	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
4.4 Bulk data exchanges use Extract Transform Load tools	Full	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. 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.
4.5 Technical diversity is controlled	Full	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
4.6 Interoperability	Full	Case Manager provides web service based integrations that use interoperable standards for data transmission. A wide range of options is available, but typically

standards must be used		data is exchanged using XML, CSV or JSON payloads
4.7 Network quality must be maintained	Full	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. 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.
4.8 Software must be deployed on an infrastructure that will enable it to perform well	Full	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.
4.9 IT systems are preferably open source	Partial	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.
4.10 Single Sign-On (SSO) must be supported	Full	Case Manager supports integration with Microsoft Active Directory through standard authentication protocols, TODO explicit protocols in here. 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
4.11 Technology capability must be established and maintained	Full	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.

4.12 Applications are delivered using open standards	Full	Case Manager is built using open standards wherever possible and IIZUKA has contributed to the development of standards. Where data is interchanged with Case Manager IIZUKA uses open standards as the formats of that data.
4.13 IT systems are scalable	Full	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. IIZUKA also conducts regular performance tests of the solution so as to ensure new developments and features do not adversely affect the solution
4.14 End-to-end security must be provided using multiple defensive strategies	Full	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. Case Manager includes a comprehensive Role Based Access Control (RBAC) model that allows control over access to both data and functions. 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. 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

4.15 Integration with external IT systems is localised in dedicated IT components	Full	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 response below) and Active Directory.

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.

Appendix G - Service Delivery Response

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

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:

Foreign and Commonwealth Office. (FCO)

Secure Case Management for 1000 users in 200+ countries – Ongoing contract. Live February 2016

Case Manager® is used by the UK's Foreign and Commonwealth's consular service to manage their case load which handles data classified as OFFICIAL:Sensitive

The FCO promotes and protects the United Kingdom's interests overseas, supporting citizens and businesses around the globe. The FCO has a worldwide network of embassies and consulates, employing over 14,000 people in nearly 270 diplomatic offices. It works with international organisations to promote UK interests and global security, including the EU, NATO, the United Nations, the UN Security Council and the Commonwealth.

The FCO needed a new system to help manage the consular side of the business, supporting British Nationals who live, work and travel overseas.

The FCO manages tens of thousands of incidents across the world every year, from lost passports and travel documents, to more involved difficulties and issues faced by UK citizens travelling, living or working abroad,

including hospitalisation, arrest, being a victim of crime and even death overseas. These incidents are managed by a combination of staff in embassies and consulates around the world working with their counterparts in the FCO in London. They needed a casework system which would work reliably and securely, across the globe via the internet, including in countries with limited infrastructure. The system also needed to integrate and communicate with other Consular systems, such as that which produces Emergency Travel Documents, as well as with new online Consular services and systems managed by other Government Departments.

Case Study at: http://www.iizuka.co.uk/case-study/fco

Pensions Ombudsman

Secure Case management for 70 users within an OFFICAL: Sensitive environment. Ongoing contract – live January 2013

They are an independent organisation set up by law to investigate complaints about pension administration.

The PO needed to modernise their case work activities to ensure that the operational legal guidelines of their work were being followed at all times by their case workers and relevant, accurate management information could be accessed easily and quickly. The data needed to be managed securely and delivered over the internet.

Appendix H - Exit/Off Boarding Response

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 flatting 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 inform 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.