Draft ANNEX 4 - IT Requirements, CMS and Business Continuity

1 DEFINITIONS AND INTRODUCTION

1.1 In this Annex, the following expressions shall have the following meanings unless the context otherwise requires and any other terms defined in the Standard Terms, the Procedure Regulations and the Specification shall, if used in this Annex, have the meaning in the Standard Terms, the Procedure Regulations and the Specification (as applicable) applied to them:

"*Approved Device*" means a device which conforms with the LAA Security Requirements document and covers both the device used to access the CHS and your CMS as well as the device that provides the telephony to make and/or receive calls;

"*Back Door Telephony*" means advice calls routed to you via Operator Service;

"Business Continuity Plan" means a plan published by the LAA setting out the processes and arrangements which you shall follow to ensure continuity of your business processes and operations following any failure or disruption of any element of the provision of Contract Work and the recovery of the provision of Contract Work in the event of an unplanned interruption;

"Business Continuity Disaster Recovery Plan" means your plan setting out the processes and arrangements which you shall follow to ensure continuity of your business processes and operations following any failure or disruption of any element of the provision of Contract Work and the recovery of the provision of Contract Work in the event of an unplanned interruption, as required by paragraph 2.3 below;

"CHS" means a Case Handling System;

"CMS" means a Case Management System*;*

"Critical Services" means the telephony infrastructure to receive and make calls and internet capability to ensure access to the CHS;

"Disaster" means an unplanned interruption (whether of information processing facilities or systems or otherwise) which significantly impairs your ability to perform Contract Work (in whole or in part) to the standard of the KPIs and/or in accordance with the other terms of the Contract This is a Severity Level 1 (as defined in Table 1 below) and if such matter is not fixed within 4 hours of occurring you shall implement your Business Continuity Plan immediately.

"Front Door Telephony" means advice calls routed directly to you via the PSTN;

"*LAA Security Requirements*" means the LAA's security requirements which are published in guidance on its website and updated from time to time;

"MOS" means the "Mean Opinion Score" being a measure of call quality;

"PSTN" means the Public Switched Telephone Network;

"Solution" means all technical components and infrastructure that are provided by you as part of and in order to effect the delivery of the CLA service. Examples of these include but are not limited to the following:

- Desktop computer;

- Telephony system including Private Branch Exchange (PBX) and any physical or virtual telephones;

- Any computer system used to store information relating to the CLA service;

- Existing IT infrastructure e.g. WAN, LAN, firewalls etc;

- Your CMS.

1.2 Below shows the major technology components of the Civil Legal Advice Specialist Advisor service at a logical level. The diagram is based on version 2.1 of the Archimate notation as defined by The Open Group.

1.3 The notation shows the current dependencies between individual components by the use of arrowed lines e.g. for the CLA client both the mobile phone and telephone components USE the PSTN. The arrows do not signify direction of flow of information. More information on the notation can be found at http://www.opengroup.org/subjectareas/enterprise/archimate-overview

1.4 The diagram also shows the current delivery responsibility for each of the logical components shown and in particular the link to the Operator Service.

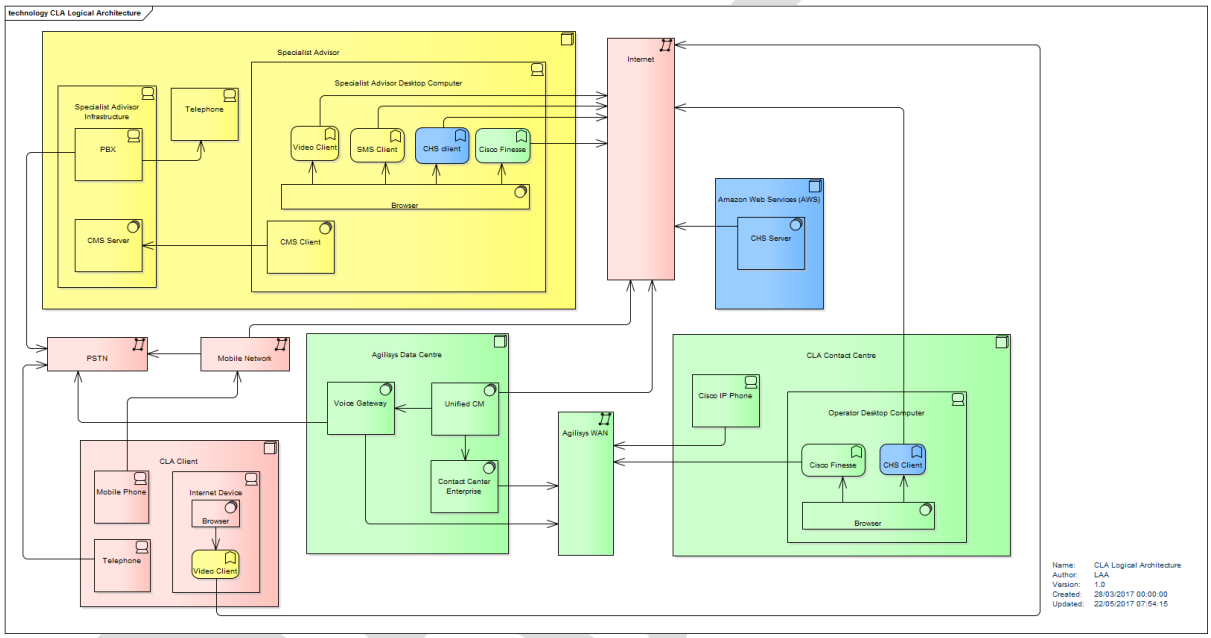

Figure 1 - CLA Logical Architecture

2. Technical Requirements

The following sections show the detailed technical requirements relating to the provision of the Specialist Advisor service as part of the CLA service. You are required to comply with all requirements and any associated guidance.

2.1 Security

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SEC-010	You shall follow the appropriate commercial good security practice & HMG/CESG guidance for security and the configuration of the Solution	
NFR-SEC-020	You shall ensure and demonstrate compliance with the LAA Data Security Requirements and LAA Data Security Guidance documents.	As part of the response to this requirement you shall complete the Compliance Statement as defined in Appendix 4 of the LAA Data Security Requirements

2.2 Integration

Requirement ID	Requirement Text	Guidance / Rationale
NFR-INT-010	The Solution shall provide a capability to send and receive emails to Clients	See clause 2.31 Annex 1 Specification
NFR-INT-020	You shall provide access to the MoJ CHS and CCMS tools for their staff	
NFR-INT-030	The Solution shall allow the following data fields to be completed based on information within a CHS record: 1. Unique reference number for Case 2. Name of organisation 3. Client Information (defined in the CLA Operations Manual 4. Category of Law 5. Matter Type Part 1 (defined in the CLA Operations Manual) 6. Matter Type Part 2 (defined in the CLA Operations Manual) 7. Date Case opened/accepted by you 8. Eligibility confirmed 9. Date Case closed by you 10. Total time spent 11. Stage Reached (defined in the CLA Operations Manual) 12. Outcome (defined in the CLA Operations Manual) 13. Level of Fixed Fee or Escape Fee 14. Total cost of Disbursements (defined in the Payments, Disbursements and Reviewing your Claims for Payments (Controlled Work) Annex)	

Requirement ID	Requirement Text	Guidance / Rationale
	15. Time spent in the current reporting month	
NFR-INT-040	The Solution shall allow a Caseworker to import all data fields specified within the CLA Operations Manual	
NFR-INT-050	You shall ensure that, where practicable, all Solution system interfaces are open and non-proprietary and adhere to Service Oriented Architecture (SOA) recognised industry best practices, principles and standards.	
NFR-INT-060	You shall ensure that, where practicable, the Solution shall support the principle of Open Architecture.	This requirement relates primarily to the development of any new components as part of this contract rather than mandating on any existing 3rd party COTS solution. As an example, in delivery of NFR-TEL-040 then any browser plug-in should be standards compliant and should not require the Client to install proprietary plug-ins.
NFR-INT-070	You shall ensure that the Solution shall provide interfaces in a manner that can be integrated using open standards or simple declared formats.	Examples of open standards include declared XML schema, declared JSON schema, agreed RESTful or SOAP web service and/or JMS

Requirement ID	Requirement Text	Guidance / Rationale
NFR-INT-080	The solution shall support the expansion of the number and type of interfaces in the future, provided the integration technology component(s) is/are appropriately licensed, and will not be artificially limited to the interfaces specified within the initial scope of the solution. You shall outline their approach to meeting this requirement.	

2.3 Service Management and Business Continuity

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SVC-010	The Solution shall support continuous normal operations during Business Hours	
NFR-SVC-020	The Solution shall be able to provide Critical Services during scheduled maintenance.	
NFR-SVC-030	You shall eliminate single points of failure and ensure that in the event of an IT service failure the service and its supporting components can be recovered rapidly to resume normal business operations.	
NFR-SVC-040	The Solution shall support an overall Service Availability of 99.9% on a monthly basis.	This is equivalent to 43.2 minutes unscheduled downtime per 30 day period. This does not apply to the scenario of catastrophic system-wide failure.
NFR-SVC-050	You shall create, by service commencement and subsequently maintain an IT Service Continuity Management model and plan that will meet the agreed service continuity and availability requirements and must ensure that this is an accurate representation of the solution.	
NFR-SVC-055	You shall ensure normal operations can be delivered within a maximum of four business hours after the occurrence of any Disaster.	
NFR-SVC-060	The Solution shall support transfer of operations between sites. We must be notified of any decision to transfer sites as soon as reasonably possible.	
NFR-SVC-080	You shall, by service commencement, create a planned maintenance	

Requirement ID	Requirement Text	Guidance / Rationale
	strategy showing the frequency and levels of maintenance required.	
NFR-SVC-090	The Solution shall deliver a Recovery Point Objective (RPO) of 30 mins.	In the event of failure being the point prior to the last uncommitted transaction each individual user logged on to the system, at the point of failure, shall not lose more than 30 minutes of data. This requirement should drive the overall resilience design for the Solution in terms of failover and backup.
NFR-SVC-100	The Solution shall support disaster recovery that utilises an arrangement of hosting in at least two geographically separate locations.	In accordance with NFR-SVC-030 above the disaster recovery site must: (a) be located such that it is not simultaneously exposed to other disasters resulting from a single event or a series of related events; and (b) not be dependent on the same physical infrastructure as supports your primary site, such that a telecommunications, LAN, server or other infrastructure failure at your primary site must not preclude you from offering service from your Disaster recovery site.
NFR-SVC-110	You shall agree a schedule with us to regularly on at least an annual basis test the backup and restore capabilities of the Solution	
NFR-SVC-120	The Solution shall provide auditable logs of backup schedules.	Auditable backup logs showing success or failure results of system backup shall be maintained and accessible
NFR-SVC-130	You shall prior to service commencement agree a Change Management process with us based on ITIL V3 principles.	

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SVC-140	You shall ensure that all staff follow agreed Change Management process.	The change management process shall apply to all services and infrastructure including but not limited to: a. Upgrades; b. Patches; c. Releases; d. Bug fixes e. Hardware upgrades; f. Capacity changes; g. Functional changes; h. Database changes; i. Key business rule changes; j. Changes introduced by new developments, programmes or projects.
NFR-SVC-150	You shall provide a minimum of 10 days' notice to us of all activities that require planned downtime.	
NFR-SVC-160	You shall provide and maintain a Definitive Software Library (DSL) of all software components and all digital CIs utilised within the Solution.	
NFR-SVC-170	You shall ensure the continuity of services to enable the continuity of the operations at all the locations designated by us for business and/or continuity purposes.	
NFR-SVC-180	You shall design, implement and regularly (at least annually) rehearse arrangements to demonstrate and ensure continuity of the service and any operational infrastructure needed to ensure the continued operation of the Solution.	
NFR-SVC-190	You shall provide prior to service commencement and subsequently maintain a Business Continuity Disaster Recovery (BCDR) Plan.	Operation of your BCDR plan must not be contingent on any individual whose role within the disaster recovery process does not have sufficient cover to ensure efficient operation due to absence or other business activities.
NFR-SVC-200	You shall ensure that their Business Continuity Disaster Recovery Plan supports the LAA's Business Continuity Plan.	

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SVC-220	You shall review the Continuity Manual at least annually and update it to take into account lessons learned relating to Continuity Management during the period since the last update.	
NFR-SVC-230	You shall notify us of any service affecting failure in accordance with Table 1, providing details of any remedial action including any re-inputting of data.	

Material or repeated failure to meet this requirement shall be deemed a Fundamental Breach

Business Continuity Timescales

Table 1 - Service Incident Notification and Fix Periods

Severity Level	Definition	Notification Period (measured from detection of problem)	Fix Period (measured from detection of problem)
1	Critical - This would be a defect which was severely affecting the Solution and the agreed contingency procedures would need to be implemented if not fixed within agreed timescales	Within 1 hour	Within 4 hours
2	High - A significant defect which means that the majority of the Solution was working as expected but there was still detrimental performance	Within 2 hours	Within 24 hours
3	Medium - A significant defect which may only be affecting a small area/number of personnel using the Solution, however this would still need to be fixed quickly	Within 2 hours	Within 48 hours
4	Low - A minor defect	Within 24 hours	ASAP - to be agreed on an individual basis

2.4 Standards

Requirement ID	Requirement Text	Guidance / Rationale
NFR-STD-010	You shall ensure that all documentation shall be produced, issued and changed in a controlled manner.	Each document, drawing or specification shall clearly state the title, author, date, issue/version and appropriate protective marking.
NFR-STD-020	You shall ensure that all documentation shall be provided electronically and in editable form in MS Word, MS Excel, MS PowerPoint, MS Visio and MS Project.	We can, without any charge, reproduce and make available the documentation for use by the Authority's staff and agents.
NFR-STD-030	All documentation shall be in the English language, and it shall use SI (Système International) units.	
NFR-STD-040	You shall ensure that all documentation conforms to agreed standards for sign off by the Authority.	
NFR-STD-050	The Solution shall adhere to OGC standards and implementation rules, where these standards and rules practically and materially benefit/optimise the solution.	
NFR-STD-060	You shall ensure that Service Management is performed in accordance with ITL v3 (2011).	
NFR-STD-080	You shall ensure that they comply with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)	From 25th May 2018 the GPDR will supersede the Data Protection Act 1998 (DPA).
NFR-STD-090	You shall ensure that they comply with the LAA Data Security Guidance (May 2016)	
NFR-STD-100	You shall ensure that they comply with the LAA Data Security Requirements (July 2016)	
NFR-STD-110	The Solution shall comply with the minimum Operating Systems and Browser requirements listed in section 3 of the LAA Remote Specialist Telephony Handbook	

2.5 Service Transition

Requirement ID	Requirement Text	Guidance / Rationale
NFR-TRA-070	You shall allow the Authority all necessary access required to monitor all testing related work carried out by you or your subcontractors	Access may be remote as well as physical access to your test facilities and includes early preparations of the test environment, test data and test tools. There shall be no limitations to the Authority's ability to access documents, plans, systems, or to meet and interview staff members or subcontractors to monitor progress not just during the testing cycles but also the early preparations for testing.
NFR-TRA-080	You shall provide prior to service commencement and subsequently maintain a Test Strategy.	The Test Strategy must include details on how and when you will prioritise the testing, preparation of the test environments, test tools, test data, and details of any significant matters outside the scope of the Provider's remit.
NFR-TRA-090	The Solution shall support dual operation alongside existing CLA Specialist Advisor contracts that either you or another third party hold.	

2.6 Performance

Requirement ID	Requirement Text	Guidance / Rationale
NFR-PRF-010	The Solution shall ensure the elapsed time between any screen rendering activity and the application being able to respond to keyboard input will be a maximum of 300ms.	The Solution should respond in a timely manner to ensure that the quality of service provided to the Client is not reduced.
NFR-PRF-020	The Solution shall ensure the elapsed time between the movement of the cursor control to the movement of the cursor on the display shall be a maximum of 100ms.	The Solution should respond in a timely manner to ensure that the quality of service provided to the Client is not reduced.
NFR-PRF-030	The Solution shall ensure a maximum of 2 seconds response time for data submission or commit in 100% of cases.	The Solution should respond in a timely manner to ensure that the quality of service provided

Requirement ID	Requirement Text	Guidance / Rationale
		to the Client is not reduced.
NFR-PRF-040	The Solution shall ensure a maximum of 2 seconds response time from request to receipt of a fully rendered Search response, for 95% of Search requests.	The Solution should respond in a timely manner to ensure that the quality of service provided to the Client is not reduced.
NFR-PRF-050	You shall ensure that all external network connections used by the Solution are sufficient for the purposes of delivering the Service.	For the avoidance of doubt, all network connections refers to any Internet, Telephony or WAN connections that are required to deliver the CLA service. Sufficient means that the connections, from all locations where the service is delivered as defined in NFR- SVC-100 have sufficient bandwidth, have no significant congestion and that any jitter or lag is minimal such that there is no detrimental impact to the CLA service received by the Client
NFR-PRF-060	You shall ensure that all Solution infrastructure is sized appropriately and is sufficient for the purposes of delivering the Service.	For the avoidance of doubt, all Solution infrastructure refers to any element of the Solution or equipment either Client, server or telephony related that is hosted either locally or within some data centre that is required to deliver the CLA service and is documented as part of the response to NFR-ITR-010. Sized appropriately means that all equipment at all locations where the service is delivered as defined in NFR- SVC-100, have enough compute, memory, disk space and network connectivity such that there is no detrimental impact to the CLA service received by the Client

Requirement ID	Requirement Text	Guidance / Rationale
NFR-PRF-070	You shall ensure that all NFRs within Annex 4 are met at all times.	Only the Authority can give any relief from any of the contractual obligations listed within this Annex.

2.7 Telephony

Requirement ID	Requirement Text	Guidance / Rationale
NFR-TEL-010	You shall ensure that different DDI numbers are used for Backdoor and Front Door telephony.	See clause 2.17 and 2.21 in Annex 1Spec 2018
NFR-TEL-020	The Solution shall not present CLI for any outbound calls.	This is to provide protection of the Client to avoid inadvertent discovery of that the Client had been in contact with the CLA e.g. to protect a Client from their partner in the case of Domestic Violence
NFR-TEL-030	The Solution shall provide voice, video and SMS based communications to the Client.	
NFR-TEL-040	You shall ensure that video services must be available over the internet via a standard internet browser	Whilst this must be browser based the download and execution of session specific plug-ins to the Client's machine will be allowed. There shall be no evidence once the browser has closed that a CLA video service was used.
NFR-TEL-050	You shall ensure that video services are secure and anonymous.	The Client should not be required to sign-up to access video services
NFR-TEL-060	You shall ensure that any DDIs used as part of Front Door Telephony or Back Door Telephony shall not be used for any other purposes.	The aim is to minimise a phone call being presented to any Caseworker inadvertently
NFR-TEL-070	The Provider shall ensure that Solution provides sufficient capacity to receive and make telephone calls via the PSTN.	Sufficient capacity means so that any person calling you in respect of Contract Work (including Clients and the Operator Service) does not receive an "all lines busy" response and are able to either speak to someone or (in the case of calls from Clients only, leave a message)

Requirement ID	Requirement Text	Guidance / Rationale
NFR-TEL-080	The Solution shall provide standard PSTN connections for telephony integration between the Provider and the Operator Service.	These may be provided using analogue, ISDN, DASS2 or other non compressed connections to mainstream recognised PSTN providers.
NFR-TEL-090	The Provider shall ensure that the Solution is capable of communicating with the communications infrastructure used by the Operator Service.	
NFR-TEL-100	The Solution shall not include any call recording functionality	
NFR-TEL-110	The Provider shall ensure that the Solution provide is able to operate in accordance with the LAA Remote Specialist Telephony Handbook	Current latest version is 7.2
NFR-TEL-120	The Provider shall ensure that the Solution provided does not degrade call quality below acceptable levels as measured by the MOS score.	MOS score should be calculated in accordance with ITU-T standards P.861 and P.862. Minimum acceptable MOS scores are 4.3 for client call originating from the PSTN and 3.9 for calls originating from a mobile network
NFR-TEL-160	The Provider shall ensure that the Backdoor telephony service is available 99.95% of time within Business Hours.	This requirement is only applicable to Provider's who provide the Backdoor telephony directly.
NFR-TEL-170	The Provider shall provide Management Information to the Authority on a monthly basis to demonstrate compliance with the Telephony related KPIs	The relevant KPIs are listed in Annex 5.

2.8 IT Requirements

Requirement ID	Requirement Text	Guidance / Rationale
NFR-ITR-010	The Provider shall provide an outline Architecture Definition Document prior to service	The ADD shall clearly show all elements of the Solution, their role, their integration within Operator Service and what Security controls are in place to protect their Solution. As a minimum the following elements within the Architecture Definition Document are required:

Requirement ID	Requirement Text	Guidance / Rationale
	commencement (ADD).	Logical Architecture - High level diagram showing all major Solution components, locations, users and interfaces with 3rd party systems e.g. CMS, Agilisys telephony, PSTN etc. together with a narrative explaining the various logical domains or layers and the components which are represented, as well as their role within the overall context of the solution. Physical Architecture - expansion of Logical Architecture to include the realisation of all the Solution components Security Architecture - showing all security controls and that provide necessary protection for Information Assets and their associated Impact Levels including any encryption technology used, the locations of devices and assumptions in regard to ownership of the network components should be included. This shall include understanding of every location that data may be held in a hosted solution to ensure compliance with security guidelines / restrictions. Network Architecture - showing how their solution is partitioned at each layer of the network, and provide details of any connectivity to other networks.
NFR-ITR-020	The Provider shall prior to service commencement provide a complete list of individual software technology components proposed for the solution.	This list will include all software components required, whether primary software packages or secondary / supporting components / frameworks. Details should be provided for each component as follows: - Product name and Vendor / OEM details; - Version number of the component proposed; - Role of the component in the solution; - Rationale for the selection of the component by the Provider; and - Any other details deemed relevant by the Provider.
NFR-ITR-030	The Provider shall prior to service commencement demonstrate how the components specified constitute a fully integrated solution, meaning where the solution is made up of more than one component part, such components are integrated together to form a	

Requirement ID	Requirement Text	Guidance / Rationale
	single, coherent, ICT solution.	
NFR-ITR-040	The Provider shall prior to service commencement provide and subsequently maintain their COTS package's technical strategy.	This shall include a timetable of planned technical component upgrades for the next three years, inclusive of any ancillary products that are planned to be incorporated into the Provider's proposed solution.
NFR-ITR-050	The Provider shall ensure that the Solution complies with the Computer Misuse Act.	This may include 'Welcome Messages' which may be shown that ensures that the Authority are compliant with this as a result of the security measures implemented.
NFR-ITR-060	The Provider shall ensure that the Solution complies with the Cabinet Office Open Standards principles.	https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles
NFR-ITR-070	The Provider shall provide prior to service commencement and subsequently maintain a Solution that meets the contractual obligation defined in Annex 1.	
NFR-ITR-080	The Provider shall provide the Solution to the Authority royalty free.	All license and maintenance costs for all Solution components shall be paid for by the Provider. No costs will be passed on to either the LAA or the Client.

2.9 Data Quality / Usability

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SYU-010	The Provider shall ensure that the CMS has been designed and configured to minimise errors in initial data entry that require additional work to correct after the Client call has ended.	This might include but is not limited to: - a reduction in the number of free text fields available and replace them with drop-down lists - use of 3rd party data validation services for items such as addresses

Requirement ID	Requirement Text	Guidance / Rationale
NFR-SYU-020	The Solution shall utilise reference data to support the entry of information (e.g. as suggested text).	
NFR-SYU-030	The Provider shall ensure the performance of the CMS is sufficient to deliver expected service to the Client	There shall be little or no lag when navigating between fields and forms within the CMS.
NFR-SYU-040	The Solution shall facilitate data sharing across its functions such that particular information is only entered once and then can be used multiple times.	
NFR-SYU-050	The Provider shall describe the approach that has been taken to ensure that the user Interface meets a high standard of usability and what objective techniques have been adopted to ensure this.	The Provider may wish to refer to design techniques that have been employed and any measurement (e.g. Provider's own or reference Heuristic Evaluation) or assurance methods utilised.
NFR-SYU-060	The Solution shall provide notifications of errors, under exception cases, in place of notices of successful completion or confirmation and in such a way as to allow the recipient(s) to directly identify from the notification the cause of the exception and to directly identify the necessary corrective action or allow the recipient to surmise the necessary corrective action.	
NFR-SYU-070	The Solution shall allow for the CMS, CHS and telephony desktop agent to be displayed simultaneously	
NFR-SYU-080	The Solution shall support the ability to format data input controls, where appropriate, to support any data validation which may be in effect.	The Provider should provide details of the types of field formatting that is utilised by the solution.
NFR-SYU-090	The Solution shall include the capability to correct data which has been entered in error. Where data is corrected, only the corrected value of a field will be made available through the solution, apart from the Audit log.	The Provider shall describe how data correction is supported in the solution.
NFR-SYU-100	The Solution shall prevent a user from retrieving incorrect data as the result of a search once it has been corrected, apart from interrogating the Audit log.	
NFR-SYU-110	The Solution shall comply with the Equality Act 2010 (c.15) in ensuring that no disabled person is at a substantial disadvantage in relation to relevant matter in comparison with	

Requirement ID	Requirement Text	Guidance / Rationale
	persons who are not disabled (Part 2, Ch 2, 20/3).	
NFR-SYU-120	The Solution shall comply with the Equality Act 2010 (c.15) in ensuring that a physical feature does not put a disabled person at a substantial disadvantage in relation to a relevant matter in comparison with persons who are not disabled (Part 2, Ch 2, 20/4).	
NFR-SYU-130	The Solution shall comply with the Equality Act 2010 (c.15) in ensuring that no disabled person would, but for the provision of an auxiliary aid, be put at a substantial disadvantage in relation to a relevant matter in comparison with persons who are not disabled (Part 2, Ch 2, 20/5).	