



www.cqc.org.uk

Contract for the Provision for Digital Hosting and Managed Service

This Contract for the provision of ICT Services includes:

Part A - Contract Data

Part B - The Schedules

Schedule 1 – Service Requirements

Schedule 2 - Service Levels

Schedule 3 – Contract Charges

Schedule 4 – Governance

Schedule 5 – Exit Management

Schedule 6 – Dispute Resolution

Schedule 8 – Customer Responsibilities and Customer Assets

Schedule 9 – Security

Schedule 10 – Records Provision

Schedule 11 – Change Control Procedure

Schedule 15– Definitions

Part C – Terms and conditions

1. Contract start date, length and methodology

2. Overriding provisions

3. Transfer and sub-contracting

4. Contractor Staff

5. Due diligence

6. Warranties, representations and acceptance criteria

7. Business continuity and disaster recovery

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

14. Data Protection and Disclosure

15. Authority Data

16. Records and audit access

17. Records and audit access

18. Freedom of Information (FOI) requests

19. Security

20. Guarantee

21. Incorporation of Terms

22. Managing Disputes

23. Termination

24. Consequences of termination

25. Contractor's status

26. Notices

27. Exit plan

28. Handover to replacement contractor

29. Force Majeure

30. Entire Agreement

31. Liability

32. Waiver and cumulative remedies

33. Fraud

34. Prevention of bribery and corruption

35. Legislative change

36. Publicity, branding, media and official enquiries

37. Non Discrimination

38. Premises

39. Equipment

40. Contracts (Rights of Third Parties) Act

- 41. Law and jurisdiction
- 42. Environmental requirement
- 43. Defined Terms
- 44. Interpretation
- 45. Management Information
- 46. Transparency and Access to Records
- 47. Relationship of the Parties
- 48. No Guarantee
- 49. Freedom of Information Act
- 50. Tax compliance.
- 51. Official Secrets Act
- 52. Subcontracting
- 53. Complaints handling and resolution
- 54. Communication
- 55. Severability

PARTIES:

- (1) THE CARE QUALITY COMMISSION of 3rd Floor, 151 Buckingham Palace Road, London, SW1W 9SZ (the "Authority");

AND

- (2) AXIS 12 LTD registered in England and Wales under number xxx whose registered office is Unit 14, The Ivories, 6-18 Northampton Street, London, N1 2HY (the "Contractor")

(each a "Party" and together the "Parties").

WHEREAS

- i. This Contract is issued by the Authority in accordance with the VEAT Notice Reference 2017-23507 dated 07/09/2017.
- ii. The Contractor is an expert in the field of digital hosting services and experienced supplier to the Authority.
- iii. This Contract is for the provision of Digital hosting and Managed services by the Contractor to the Authority.

Formation of Contract

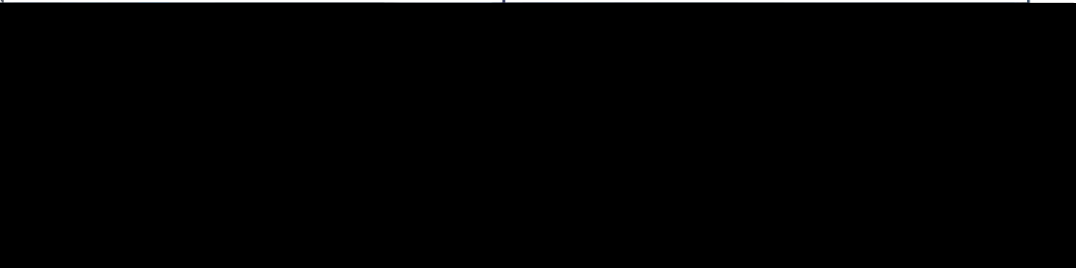
1.1 By signing and returning this the Contractor agrees to enter into a Contract with the Authority comprising of the following documents, which in the event of conflict shall be interpreted with the following order of precedence:

- 1.1.1 Part A – The Contract Data
- 1.1.2 Part B – The Schedules
- 1.1.3 Part C – The Terms and Conditions

1.2 The Parties agree that they have read the Contract Data, the Schedules and the Terms and Conditions by signing below and agree to be bound by this Contract upon signature by both Parties.

1.3 The terms and conditions of the Contract and Contract Data will supersede those of the Contractor Terms and Conditions.

SIGNED:

	Contractor:	Authority:
Name:		
Title:		
Signature:		
Date:		

Part A - Contract Data

Contract ref.	CQC ICTC 722
Contract title	Digital Hosting and Managed Service
Contract description	Digital Hosting and Managed Service
Start date	01/11/2017
End date	This Contract shall expire on: 1.2.1 31/10/2018; or 1.2.2 where the Customer exercises the option to extend the Agreement for a further 12 months, by giving three (3) months' notice in writing to the Contractor prior to 31/10/2018, the second (2) anniversary of the Commencement Date.
Contract value	Year one £362,064 Year two (if extended) £362,064
Charging method	Monthly
Purchase order No.	TBC

Principle contact details

Authority

From: the Authority Name: [REDACTED]
Address: 151 Buckingham Palace Road, London, SW1W 9SZ
Phone: [REDACTED]
e-mail: [REDACTED]

To: the Contractor Name: [REDACTED]
Address: Unit 14, The Ivories, 6-18 Northampton Street, London, N1 2HY
Phone: [REDACTED]
e-mail: [REDACTED]

Together: the "Parties"

Contract term

Commencement date: This Contract commences on 1st October 2017 and is valid for 12 months.

Termination: In accordance with Contract clause 23 the notice period required for Termination is at least 90 working 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.

Authority contractual details

This Contract is for the Services outlined below. It is acknowledged by the Parties that the volume of the Services utilized by the Authority may vary from time to time during the course of this Contract, subject always to the terms of the Contract.

- Services required:**
- Digital Hosting Services
 - Digital Managed Services
 - This Contract is for the provision of Services according to the technology code of practice (<https://www.gov.uk/service-manual/technology/code-of-practice.html>)
 - according to the government service design manual (<https://www.gov.uk/service-manual>) including:

Additional Services:	Not used
Location:	Services will be performed at Suppliers location, not CQC premises
Quality standards:	ISO 27001 certification for supplier and any hosting provider All supplier staff to have current CRB checks
Technical standards	No PSN requirements are needed
On-boarding	Not used
Off-boarding	See Schedule 5
Limit on supplier's liability:	In accordance with Contract clause 31.5
Insurance:	<p>Minimum Insurance Period</p> <p>Six (6) Years following the expiration or earlier termination of this Agreement</p> <p>To comply with its obligations under this Agreement and as a minimum, where requested by the Customer in writing the Contractor shall ensure that:</p> <ul style="list-style-type: none"> - professional indemnity insurance is held by the Contractor and by any agent, Sub-Contractor or consultant involved in the supply of the Services and that such professional indemnity insurance has a minimum limit of indemnity of five million pounds sterling (£5,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time; - employers' liability insurance with a minimum limit of ten million pounds sterling (£10,000,000) or such higher minimum limit as required by Law from time to time; and - public liability insurance is held by the Contractor and by any agent, Sub-Contractor or consultant involved in the supply of the Services and that such public liability insurance has a minimum limit of [REDACTED] for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time;

Authority's Responsibilities	The Authority is responsible for (See Schedule 8)
Authority's equipment	The Authority's equipment to be used in connection with this Contract includes (see Schedule 8).
Contractor's Information	
Subcontractors / Partners:	The following is a list of the Contractor's Subcontractors/Partners: <ul style="list-style-type: none"> •
Contract Charges and payment	The 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 Contract is BACS.
Payment profile:	The payment profile for this Contract is monthly in arrears.
Invoice details:	The Contractor shall issue electronic invoices monthly in arrears. In accordance with Contract clause 8, the Authority will pay the Contractor 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	All invoices must include a Purchase Order Number.
Invoice frequency	Invoice will be sent to the Authority monthly.
Contract value:	The value of this Contract is £362,064.00
Contract Charges:	See Schedule 3.

**Performance
of the service
and
deliverables**

The Contractor shall deliver the Services so as to achieve the Service Levels set out in Schedule 1 and 2.

**Collaboration
agreement**

The Authority does not require the Contractor to enter into a Collaboration Agreement.

**Warranties,
representations**

As per Contract clause 6

Part B - The Schedules

Schedule 1 Service Requirements

Services:

The Supplier shall deliver the Services to CQC in accordance with the details specified in the following:

- a) Part A of this Services section- the CQC Specification issued within the Invitation-to-Tender; this details CQC's requirements.
- b) Schedule 10a and 10b of this Agreement- the Supplier's Solution submitted to CQC on 11/01/2016 via the e-tendering portal Delta e-sourcing; this document details the methodology, staff and standards that the Suppliers will undertake in order to meet Part A.

In the event of any conflict relating to the Services detailed within this Agreement, the conflict shall be resolved in accordance with the following order of precedence:

- a) Part A- the CQC Specification.
- b) Schedule 10a and 10b- the Supplier's Solution.

Any conflict shall be resolved in accordance with the overarching Framework Terms and Conditions.

Part A- CQC Specification- the following describes the services to be provided:

Lot 2: PaaS: CQC Digital Hosting

Hosting services are required by CQC to:

- Provide information to the public via an online presence (public website)
- Provide online transactions for providers (Provider Portal)
- Support third-party digital services
- Publish our statutory register of services.

The objectives of the Digital Hosting Element are:

- Select and contract with a supplier to provide transition and hosting of the CQC online presence
 - CQC website
 - CQC online communities
 - CQC Provider Portal
- Implement the new services before the corresponding transition period of the contracts end
- Provide an uninterrupted service during the process of transition to the new service, and thereafter
- Provide best value for money, secure and performant infrastructure solution for hosting CQC websites
- Provide a platform that allows CQC to deploy and maintain software

Overview of the Current Solutions:

CQC main public facing Website- www.cqc.org.uk

The purpose of this website is to disseminate information to the public about the standard of care provided in hospitals, care homes, dental surgeries and other registered care providers. A large part of the website is a directory of 100K+ care services, which is updated currently on a daily basis.

- The site receives approximately 4.7 million page views a month – a figure that's steadily growing.
- The site runs off a database-driven content management system (CMS) known as Drupal 7, in combination with several layers of caching and the EdgeCast Content Delivery Network (CDN). A full list of software currently used to support the delivery of the website is listed in Appendix A.
- The Drupal CMS reads from two distinct databases: its own Drupal database, and a

separate MongoDB database. All directory information is stored in MongoDB in a key-value structure.

- Data is fed via an external Enterprise Service Bus, built using MuleSoft ESB.
- The search facility is powered by an external Solr service.
- The website uses an external messaging service ElasticEmail to send email alerts to members of the public.
- The site uses multiple database and web servers, and multiple layers of software and hardware caching to achieve its required performance.
- Neither the general public nor providers or care services are able to log into the site (i.e. the vast majority of the site's users are anonymous).

CQC online communities websites

These two websites are dedicated to interacting with the public (<https://communities.cqc.org.uk/public/>) and healthcare providers (<https://communities.cqc.org.uk/provider/>) and gathering their views on subjects related to how CQC operates.

- The two websites can be accessed by authenticated users only. The public website has 2580 and the provider website has 9303 active users (as of June 2015).
- The websites were built using the Drupal 7 Commons distribution. They have then been configured and slightly customised. Both sites share the same codebase and have separate databases. There is a caching layer, but no CDN.
- The websites contain sensitive data and require IL2 hosting.
- The websites use an external messaging service ElasticEmail to send emails to their users.

CQC Provider Portal– <https://services.cqc.org.uk/>

The Provider Portal is a web-based platform that allows the providers that CQC regulates to carry-out transactions online. CQC regulates approximately 30,000 providers who submit around 420,000 forms per annum. These transactions fall into broadly into two main types:

- 1) Registration variations
- 2) Statutory notifications

The Portal has been used by GPs since October 2013, to carry out variations to their registration. High-volume statutory notifications went live in April 2015 and Provider Portal accounts have recently been rolled out to other sectors.

The Portal is built on Drupal 7 and integrates with internal systems via a Java/PostgreSQL-based middleware layer (out of scope for this proposal).

Infrastructure Requirements

CQC Volumetric Specification

The following volumetrics provide an overview of CQC's scope

CQC require the ability to add and remove infrastructure within 10 working days as required due to increase or decrease in volumetrics

ID	Requirement	CQC website	Online communities	Provider Portal
IR1.1	Number of documents*	170,167	231	N/A
IR1.2	Number of image files *	22,262	1,857	N/A
IR1.3	Number of video files *	0	0	N/A
IR1.4	Number of audio files *	33	0	N/A
IR1.5	Average total site visits per month **	3,500,000	<5,000	11,664
IR1.6	Peak site visits per day **	155,000	<1,000	892
IR1.7	Average Page Impressions per month **	4.8 mil	<20,000	98,928
IR1.8	Number of unique editors	6	2	1
IR1.9	Average Search Requests per month **	750,000	N/A	N/A
IR1.10	CDN traffic requirement per month **	1.1 TB	N/A	N/A
IR1.11	Backup tape storage requirement per	1 TB	10GB	1 TB

	month **			
IR1.12	Number of Provider Portal user accounts activated (total)***	N/A	N/A	7,000 (14,000, 250,000)
IR1.13	Number of Provider Portal online transactions per month****	N/A	N/A	2,000 (4,000, 40,000)

* on 15 July 2015

** For April/May/June 2015

*** Provider Portal accounts rolled out to all sectors. The first figure is for number of accounts at the end of June 2015. The second figure is an estimate of the number of accounts expected by 31 December 2015 and the third figure is the maximum currently anticipated.

**** Monthly online transaction. The first figure is for June 2015, the second is an estimate for December 2015 and the third figure is the likely maximum number of transactions.

Required Service Availability and Continuity (up to and including OS level)

ID	Availability Metric	Monthly Target
IR2.1	Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%
IR2.2	Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%
IR2.3	Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%
IR2.4	Non-Live environments to be available during standard business hours	99.0%
IR2.5	Non-Live environments to be available outside standard business hours	95.0%
IR2.6	In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours	100%

Service Performance

These conform to the standard measures as implemented by www.newrelic.com

ID	Performance Metric	Monthly Target
IR3.1	App server Apdex T-value 0.5 seconds	0.96
IR3.2	Browser Apdex T-value 7 seconds	0.98

Environments Infrastructure

Provision of hardware, software and support up to and including OS level

ID	Requirement	CQC website	Online communities	Provider Portal
IR4.1	A hosted Drupal 7 platform with the following instances: a) Development environment b) Test environment c) Production environment d) Disaster recovery environment e) Staging environment f) Additional testing environment	a, b, c, d	a, c	a, b, c, d, e, f
IR4.2	The solution must provide a high availability: a) MySQL database b) MongoDB database	a, b	a	a, b
IR4.3	The solution must provide a caching	a, b, c	b, c	N/A

	service: a) CDN cache b) Page furniture cache (e.g. Nginx) c) HTML and search cache (e.g. Varnish)			
IR4.4	Disaster recovery - The solution must provide a high availability	H	H	H
IR4.5	Load balancing - There should be no single point of component failure, so load balancing should be deployed where necessary to balance requests.	H	H	H
IR4.6	The sites must continue to integrate with: a) Elastic Email b) Axis12 Find service (Solr) c) CQC ESB d) Google maps e) Google places f) Google geo-code g) Checkbox h) OpenAM	a, b, c, d, e, f	a	c, h

ta Centre

ID	Requirement
IR5.1	Hosting environment must be certified to IL2 for Online communities and Provider Portal
IR5.2	Data Centre to have classification of at least Tier III from the Uptime Institute or alternative comparable classification
IR5.3	All elements of the hosting solution must physically exist within the European Union
IR5.4	External and internal access to environments should be via firewalls

Migration

ID	Requirement
IR6.1	Migration design required - The Supplier must utilise as much as, if not all, software configuration and development (code base) from the previous solution, ideally in a "lift and shift" approach. Redevelopment and bespokeing must be kept to a minimum and must be expressly identified in the solution
IR6.4	Security testing
IR6.5	Documentation - Technical Architecture required Transparency on hosting resources and design will be shared with CQC

Development Features

The ability for CQC to perform these tasks in all environments is required

ID	Requirement
IR7.1	No ability to SHH to any environments

Service Management Requirements:

Service and Support KPI's

ID	Category	Service Level Measurement	Monthly Service Level Target
SM1.1	Incident and Problem Management	Incidents logged through a Service Desk channel acknowledged immediately	100%
SM1.2		Severity 1 incidents resolved within 2 hours of logging the incident. During the investigation updates to be provided every 15 min and root cause of incident reported within 24 hours of incident resolution	100%
SM1.3		Severity 2 incidents resolved within 6 business hours of logging the incident	100%
SM1.4		Severity 3 incidents resolved within 2 business days of logging the incident	95%
SM1.5		Severity 4 incidents resolved or closed (and corresponding problem record created) within 5 business days of logging the incident	95%
SM1.6		All incidents to be resolved within 20 business days	100%
SM1.7	Service Management	Service reports and plans circulated in accordance with defined schedule unless otherwise agreed between the parties	100%
SM1.8		Service requests logged through a Service Desk channel acknowledged within 30 min	100%
SM1.9		Impact assessment for Service Requests delivered within 3 business days	100%
SM1.10		Service requests completed and closed within timescales agreed as part of Impact Assessment process	100%

Security

ID	Requirement
SM2.1	Supplier must hold a current ISO27001 certificate with the British Standards Institution
SM2.2	All employees with access to IL2 data on the hosting environment must have undergone appropriate security screening that can be evidenced if requested

Support

ID	Requirement
SM3.1	Infrastructure monitoring Provision of detailed server side monitoring, tracking resource consumption and ability to set alarms and send emails and text messages when configurable thresholds are met.
SM3.2	Ticketing system to raise and track requests/issues
SM3.3	Performance testing - The solution must be able to allow for meaningful and consistent performance testing

Service Management Plans Required at Commencement of Service

ID	Purpose
SM4.1	Service Continuity - To show what processes the Supplier has in place to safeguard the continuity of the business
SM4.2	Availability - To detail how the availability SLA(s) will be met including reference to Disaster Recovery arrangements and how this would support the attainment of the SLA.
SM4.3	Capacity - To detail how the Supplier will monitor and manage capacity, in terms of people, ability to meet traffic volumes, etc.
SM4.4	Change Management - To detail how the Supplier will manage the integration of changes to services so that the organisation has minimal disruption
SM4.5	Incident Escalation - To detail the process for escalating incident severity – e.g. who to contact and how. Also to detail how CQC will be kept updated.
SM4.6	Severity 1 incident - To detail how severity 1 incidents will be managed to ensure the incident resolution SLA can be achieved

Service Management Reports

ID	Name of report / Frequency	Purpose
SM5.1	Release schedule / Updated weekly	Details of all service fixes to be implemented and release dates
SM5.2	Major incidents action point log / Monthly and ad hoc based on request	Detail action points raised at major incident reviews and tracks them to resolution
SM5.3	Monthly incident report / Monthly	Details all open incidents with details of progress towards resolution
SM5.4	Service requests status report / Monthly and ad hoc	Details status of all open Service Requests and intended implementation

Support time

The costs of supporting the solution up to and including OS level should be included in the proposal. Any request by CQC that is deemed outside of this scope should be approved first before executed and changed for.

Incident Management Categorisation

The following is the required categorisation of incidents; suppliers should state any deviations from these in the service management offered by the solution.

Severity 1: Impact = Critical

Functional	Total or partial apparent loss or significant degradation of the performance of the solution
------------	--

	A large number of Users or End Users are unable to access the solution or part of the solution
Security	A security breach has been detected and remains critical until its impact is known
	A new or unknown virus has been detected and remains critical until its impact is known and the Incident is re-classified if appropriate
	Targeted attack
	Non-targeted attack
	Loss of data affecting the security of the network, infrastructure of systems
	Theft/loss of cryptography equipment or media
	DoS/DDos – successful
	AV alert/quarantine – widespread
	Loss of public online service
	Unauthorised access
	Damaging unauthorised changes to system hardware
	Phishing (fraud involving misuse of branding).

Severity 2: Impact = Serious

Functional	A small number of Users or End Users are unable to use the solution or part of the solution as normal and they are carrying out time critical business activities
	Performance is significantly degraded but the Solution is still usable.
Security	DoS/DDos – unsuccessful
	Network monitoring alert
	Employee abuse of privileges or security policy (e.g. emailing login credentials).

Severity 3: Impact = Minor

Functional	A small number of Users or End Users are unable to use the solution or part of the solution as normal. No time critical business activities are affected
	Performance is slightly degraded but the Solution is still usable
Security	AV alert/quarantine – single

Severity 4: Impact = Low

Functional	The Solution or part of the Solution does not perform as expected by the User but does not prevent the User from performing time critical business activities and the Solution or part of the Solution does not fail. Processing completes as required. A workaround is available and/or planned. No critical processing is affected. These Incidents are characterised as 'irritants' and may be closed as Incidents and logged as a corresponding problem
Security	None defined

Appendix A

Current Hosting Infrastructure

Public Site

Component		Development	Test	Production (Live)	Production (DR)
Location		Ash	Ash	Newbury	AWS
Security rating		IL2	IL2	IL2	IL0
Web	Drupal 7	1 x 1 unit	2 x 1 units	3 x 2 units	3 x 2 units
DB	MySQL	1 x 1 unit	1 x 1 units	1 x 4 units	1 x 4 units
Caching	Varnish	Shared (staging)	Shared (staging)	Shared (production)	Shared (production)
Search	Solr	Y	Y	Y	Y
CDN	Edgecast	N	N	Y	Y
Monitoring	New Relic	N	N	Y	Y
	Zenoss	Y	Y	Y	Y
IDS	Snort	N	N	Y	N
Backups	Location	-	-	S3	-
	Timing	-	-	00:00	-
DNS	Management	Customer's ISP	Customer's ISP	Customer's ISP	Customer's ISP
	Owner	Customer	Customer	Customer	Customer
URLs	Production (Live + DR)	cqc.org.uk			
	Test	test.cqc.org.uk			
	Dev	dev.cqc.org.uk			
Disaster recovery	RPO	-	-	24hrs	-
	RTO	-	-	15mins	-
Tools	Jenkins	Y	Y	N	N
	New Relic	N	N	Y	Y

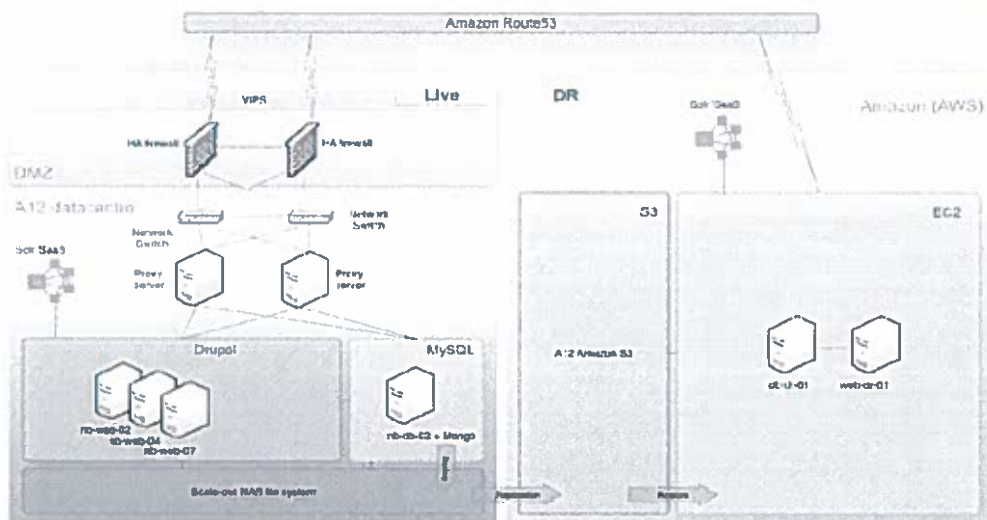
Community Sites

Component		Development	Test	Production (Live)	Production (DR)
Location		Ash	-	Ash	-
Security rating		IL2	-	IL2	-
Web	Drupal 7	1 x 1 unit	-	2 x 2 units	-
DB	MySQL	1 x 1 unit	-	1 x 2 units	-
Caching	Varnish	Shared (staging)	-	Shared (production)	-
Search	Solr	N	-	N	-
CDN	Edgecast	N	-	N	-
Monitoring	New Relic	N	-	N	-
	Zenoss	Y	-	Y	-
IDS	Snort	N	-	N	-
Backups	Location	-	-	S3	-
	Timing	-	-	00:00	-
DNS	Management	Route53	-	Route53	-
	Owner	Axis12	-	Axis12	-
URLs	Production (Live + DR)	cqccomms.co.uk communities.cqc.org.uk/provider/ communities.cqc.org.uk/public/			
	Test	-			
	Dev	dev-communities.axis12.com/public/ dev-communities.axis12.com/public/			
Disaster recovery	RPO	-	-	-	-
	RTO	-	-	-	-
Tools	Jenkins	N	-	N	-
	New Relic	N	-	N	-

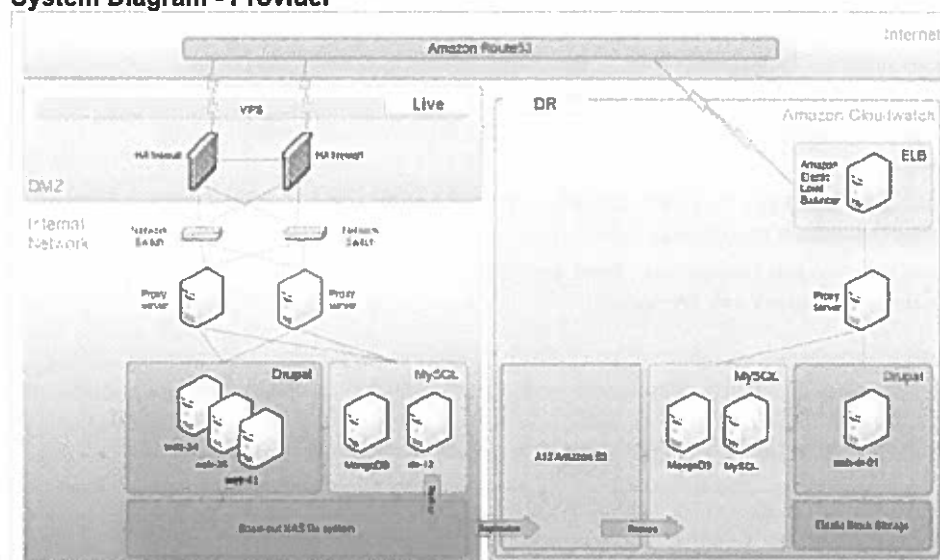
Provider Portal

Component		Dev01 Dev02	Test01 Test02	Staging	Production (Live)	Production (DR)
Location		Ash	Ash	Ash	Ash	AWS
Security rating		IL2	IL2	IL2	IL2	IL0
Web *	Drupal 7	3 units	3 units 3 units	4 units	6 units	6 units
DB *	MySQL	2 units	2 units	4 units	4 units	4 units
Loadbalancing	HAP	1 x 2 units	1 x 2 units	4 x 2 units	4 x 2 units	1 x 2 units
Caching	Varnish	Shared	Shared	Shared	Shared	Shared
Search	Solr	N	N	N	N	N
CDN	CloudFront	N	N	N	N	N
Monitoring	New Relic	N	N	N	Y	Y
	Zenoss	Y	Y	Y	Y	Y
IDS	Snort	N	N	N	N	N
Backups	Location	-	-	-	S3	-
	Timing	-	-	-	00:00	-
DNS	Management	Route53	Route53	Route53	Route53	Route53
	Owner	Axis12	Axis12	Axis12	Axis12	Axis12
URLs	Production (Live + DR)	https://services.cqc.org.uk http://authservices.axis12.com				
	Staging	https://staging.services.cqc.org.uk				
	Test	https://test01.services.cqc.org.uk https://test02.services.cqc.org.uk				
	Dev	https://dev01.services.axis12.com https://dev02.services.axis12.com				
Disaster recovery	RPO	-	-	-	-	24hrs
	RTO	-	-	-	-	30mins
Tools	Jenkins	N	N	N	N	N
	New Relic	N	N	N	N	N

System diagram



System Diagram - Provider



CQC Digital Hosting Managed Service

Support services are required by CQC to:

- Provide information to the public via an online presence (public website)
- Provide online transactions for providers (Provider Portal)
- Support third-party digital services
- Publish our statutory register of services.

The objectives of the Digital Hosting Element are:

- Select and contract with a supplier to provide transition and hosting of the CQC online presence
 - CQC website
 - CQC online communities
 - CQC Provider Portal
- Implement the new services before the corresponding transition period of the contracts end
- Provide an uninterrupted service during the process of transition to the new service, and thereafter
- Provide best value for money, secure and performant infrastructure solution for hosting CQC websites
- Provide a platform that allows CQC to deploy and maintain software

Overview of the Current Solutions:

CQC's main public facing website – www.cqc.org.uk

The purpose of this website is to disseminate information to the public about the standard of care provided in hospitals, care homes, dental surgeries and other registered care providers. A large part of the website is a directory of 100K+ care services, which is updated currently on a daily basis.

- The site receives approximately 4.7 million page views a month – a figure that's steadily growing.
- The site runs off a database-driven content management system (CMS) known as Drupal 7, in combination with several layers of caching and the EdgeCast Content Delivery Network (CDN). A full list of software currently used to support the delivery of the website is listed in Appendix A.
- The Drupal CMS reads from two distinct databases: its own Drupal database, and a

separate MongoDB database. All directory information is stored in MongoDB in a key-value structure.

- Data is fed via an external Enterprise Service Bus, built using MuleSoft ESB.
- The search facility is powered by an external Solr service.
- The website uses an external messaging service ElasticEmail to send email alerts to members of the public.
- The site uses multiple database and web servers, and multiple layers of software and hardware caching to achieve its required performance.
- Neither the general public nor providers or care services are able to log into the site (i.e. the vast majority of the site's users are anonymous).

CQC online communities websites

These two websites are dedicated to interacting with the public (<https://communities.cqc.org.uk/public/>) and healthcare providers (<https://communities.cqc.org.uk/provider/>) and gathering their views on subjects related to how CQC operates.

- The two websites can be accessed by authenticated users only. The public website has 2580 and the provider website has 9303 active users (as of June 2015).
- The websites were built using the Drupal 7 Commons distribution. They have then been configured and slightly customised. Both sites share the same codebase and have separate databases. There is a caching layer, but no CDN.
- The websites contain sensitive data and require IL2 hosting.
- The websites use an external messaging service ElasticEmail to send emails to their users.

CQC Provider Portal– <https://services.cqc.org.uk/>

The Provider Portal is a web-based platform that allows the providers that CQC regulates to carry-out transactions online. CQC regulates approximately 30,000 providers who submit around 420,000 forms per annum. These transactions fall into broadly into two main types:

- 1) Registration variations
- 2) Statutory notifications.

The Portal has been used by GPs since October 2013, to carry out variations to their registration. High-volume statutory notifications went live in April and Provider Portal accounts are currently being rolled out to other sectors. This should be completed by the end of 2015.

The Portal is built on Drupal 7 and integrates with internal systems via a Java/PostgreSQL-based middleware layer (out of scope for this proposal).

Requirements:

Service Availability and Continuity (above OS level)

ID	Availability Metric	Monthly Target
IR2.1	Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%
IR2.2	Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%
IR2.3	Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%
IR2.4	Non-Live environments to be available during standard business hours	99.0%
IR2.5	Non-Live environments to be available outside standard business hours	95.0%
IR2.6	In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours	100%

Service Performance

These conform to the standard measures as implemented by www.newrelic.com

ID	Performance Metric	Monthly Target
IR3.1	App server Apdex T-value 0.5 seconds	0.96
IR3.2	Browser Apdex T-value 7 seconds	0.98

Environments Infrastructure

Provision of software and support above OS level is in scope of this tender

ID	Requirement	CQC website	Online communities	Provider Portal
IR4.1	A hosted Drupal 7 platform with the following instances: g) Development environment h) Test environment i) Production environment j) Disaster recovery environment k) Staging environment l) Additional testing environment	a, b, c, d	a, c	a, b, c, d, e, f
IR4.2	The solution must provide a high availability: c) MySQL database d) MongoDB database	a, b	a	a, b
IR4.3	The solution must provide a caching service: d) CDN cache – CQC already has a direct arrangement with EdgeCast e) Page furniture cache (e.g. Nginx) f) HTML and search cache (e.g. Varnish)	a, b, c	b, c	N/A
IR4.4	Disaster recovery - The solution must provide a high availability	H	H	H
IR4.5	The sites must continue to integrate with: i) Elastic Email j) Axis12 Find service (Solr) k) CQC ESB l) Google maps m) Google places n) Google geo-code o) Checkbox p) OpenAM	a, b, c, d, e, f	a	c, h

Migration

ID	Requirement
IR6.1	Migration design required - The Supplier must utilise as much as, if not all, software configuration and development (code base) from the previous solution, ideally in a "lift and shift" approach. Redevelopment and bespokeing must be kept to a minimum and must be expressly identified in the solution
IR6.2	Deployment support required

IR6.3	System integration testing
IR6.4	Security and Penetration testing

Development Features

The ability for CQC to perform these tasks in all environments is required

ID	Requirement
IR7.1	Ability to copy databases from Production to non-Production environments
IR7.2	Ability to download databases and assets to create local dev environments
IR7.3	Have full access to all code repositories and branches
IR7.4	Ability to deploy code to all environments
IR7.5	No ability to SSH to any environments

Service and Support KPI's

ID	Category	Service Level Measurement	Monthly Service Level Target
SM1.1	Incident and Problem Management	Incidents logged through a Service Desk channel acknowledged immediately	100%
SM1.2		Severity 1 incidents resolved within 2 hours of logging the incident. During the investigation updates to be provided every 15 min and root cause of incident reported within 24 hours of incident resolution	100%
SM1.3		Severity 2 incidents resolved within 6 business hours of logging the incident	100%
SM1.4		Severity 3 incidents resolved within 2 business days of logging the incident	95%
SM1.5		Severity 4 incidents resolved or closed (and corresponding problem record created) within 5 business days of logging the incident	95%
SM1.6		All incidents to be resolved within 20 business days	100%
SM1.7	Service Management	Service reports and plans circulated in accordance with defined schedule unless otherwise agreed between the parties	100%
SM1.8		Service requests logged through a Service Desk channel acknowledged within 30 min	100%
SM1.9		Impact assessment for Service Requests delivered	100%

		within 3 business days	
SM1.10		Service requests completed and closed within timescales agreed as part of Impact Assessment process	100%

Security

ID	Requirement
SM2.1	Supplier must hold a current ISO27001 certificate with the British Standards Institution
SM2.2	All employees with access to IL2 data on the hosting environment must have undergone appropriate security screening that can be evidenced if requested

Support

ID	Requirement
SM3.1	Support for out of hours releases required
SM3.2	Web monitoring Provision of log monitoring, ability to set alarms and send emails and text messages when configurable thresholds are met and/or events occur. Monitoring service must monitor all components of the solution, including Web, DB, Varnish, external connections (Solr, ESB). Full access to reporting must be enabled.
SM3.3	Ticketing system to raise and track requests/issues
SM3.4	Backup and restore services to and from tape are required at least one a day
SM3.5	Performance testing - The solution must be able to allow for meaningful and consistent performance testing

Service Management Plans Required at Commencement of Service

ID	Purpose
SM4.1	Service Continuity - To show what processes the Supplier has in place to safeguard the continuity of the business
SM4.2	Availability - To detail how the availability SLA(s) will be met including reference to Disaster Recovery arrangements and how this would support the attainment of the SLA.
SM4.3	Capacity - To detail how the Supplier will monitor and manage capacity, in terms of people, ability to meet traffic volumes, etc.
SM4.4	Change Management - To detail how the Supplier will manage the integration of changes to services so that the organisation has minimal disruption
SM4.5	Release and Deployment - To detail how the Supplier will manage the integration of releases and deployments so that the organisation has minimal disruption
SM4.6	Incident Escalation - To detail the process for escalating incident severity – e.g. who to contact and how. Also to detail how CQC will be kept updated.
SM4.7	Severity 1 incident - To detail how severity 1 incidents will be managed to ensure the

	incident resolution SLA can be achieved
--	---

Service Management Reports

ID	Name of report / Frequency	Purpose
SM5.1	Release schedule / Updated weekly	Details of all developments and service fixes to be implemented and release dates
SM5.2	Major incidents action point log / Monthly and ad hoc based on request	Detail action points raised at major incident reviews and tracks them to resolution
SM5.3	Monthly incident report / Monthly	Details all open incidents with details of progress towards resolution
SM5.4	Service requests status report / Monthly and ad hoc	Details status of all open Service Requests and intended implementation

Support time

9 days per month will be provided to the supplier to maintain the solution.

10 days per month will be provided to the supplier for ad-hoc support requests. Those days will not be transferable to the following month if unused.

Incident Management Categorisation

The following is the required categorisation of incidents; suppliers should state any deviations from these in the service management offered by the solution.

Severity 1: Impact = Critical

Functional	Total or partial apparent loss or significant degradation of the performance of the solution
	A large number of Users or End Users are unable to access the solution or part of the solution
Visual	<p>An element of Content is visually or perceptually incorrect across a large portion of the solution and the incident cannot be resolved by re-publishing the relevant appropriate Content</p> <ul style="list-style-type: none"> This element is highly visible and immediately observable on current or popular versions of browsers and detracts from the overall perception of the solution. This element would prevent certain categories of Users or End Users from using the Solution The End User reaction to this element would be negative and lead to adverse comment or non-use of the relevant Solution
Content	Non defined at present
Security	A security breach has been detected and remains critical until its impact is known
	Targeted attack
	Non-targeted attack
	Loss of data affecting the security of the network, infrastructure of systems
	Theft/loss of cryptography equipment or media
	DoS/DDos – successful
	Loss of public online service
	Unauthorised access
	Damaging unauthorised changes to system hardware
	Phishing (fraud involving misuse of branding).

Severity 2: Impact = Serious

Functional	A small number of Users or End Users are unable to use the solution or part
------------	---

	of the solution as normal and they are carrying out time critical business activities
	Functionality fails to comply with agreed functional specification in a manner that renders the functionality unusable for its intended business use
	Performance is significantly degraded but the Solution is still usable.
Visual	<p>An element of Content is visually or perceptually incorrect across some page instances of the Solution and the Incident cannot be resolved by re-publishing the relevant appropriate Content</p> <ul style="list-style-type: none"> • This element is visible or observable on current or popular versions of browsers and detracts from the overall perception of the Solution. • This element would impair the use of the Solution by certain categories of users • The End User reaction to this element would be that the design of the Solution was poor and lead to adverse comment
Content	The appearance of Content which would cause a user to misinterpret the Content owner's intention
Security	Website defacement
	DoS/DDos – unsuccessful
	Employee abuse of privileges or security policy (e.g. emailing login credentials).

Severity 3: Impact = Minor

Functional	<p>A small number of Users or End Users are unable to use the solution or part of the solution as normal. No time critical business activities are affected</p> <p>Performance is slightly degraded but the Solution is still usable</p> <p>Any repeatable issue to do with functionality such that it fails to comply with its agreed functional specification in a manner that does not render it unusable for its intended business use (e.g. spurious characters in an alert)</p> <p>Any fault in internal functionality of the Solution not visible to End Users (e.g. broken links report, enhanced feedback handling).</p>
Visual	<p>An element of Content is visually or perceptually incorrect across some page instances of the Solution and the Incident cannot be resolved by re-publishing the relevant appropriate Content</p> <ul style="list-style-type: none"> • This element is visible or observable on a number of browsers and versions within scope, but is not immediately noticeable and detracts from the overall perception of the Solution. • This element would cause inconvenience to certain End Users or categories of End users • The End User reaction to this element once noticed may be poor but would not prevent use or return to the Solution
Content	Any Content related issue that is deemed by the originator to be sufficiently embarrassing that it should not wait until next release
Security	Spam

Severity 4: Impact = Low

Functional	<p>The Solution or part of the Solution does not perform as expected by the User but does not prevent the User from performing time critical business activities and the Solution or part of the Solution does not fail. Processing completes as required. A workaround is available and/or planned. No critical processing is affected. These Incidents are characterised as 'irritants' and may be closed as Incidents and logged as a corresponding problem</p> <p>One-off errors where functionality fails to comply with its agreed functional specification</p> <p>User queries 'How can I?' questions</p>
------------	--

Visual	<p>An element of Content is visually or perceptually incorrect across some page instances of the Solution and the Incident cannot be resolved by re-publishing the relevant appropriate Content</p> <ul style="list-style-type: none"> This element is visible or observable on certain browsers and versions within scope under some conditions but not to the majority of End Users This element would cause annoyance or inconvenience to a small section of End Users
Content	Incidents where it is acceptable to wait until the next scheduled release for a fix (e.g. trivial spelling, punctuation mistake or appearance which does not affect the sense of the Content). Workarounds to P2 and P3 Incidents
Security	None defined

Appendix A

QC Volumetrics

The following volumetrics provide an overview of CQC's scope

ID	Requirement	CQC website	Online communities	Provider Portal
IR1.1	Number of documents*	170,167	231	N/A
IR1.2	Number of image files *	22,262	1,857	N/A
IR1.3	Number of video files *	0	0	N/A
IR1.4	Number of audio files *	33	0	N/A
IR1.5	Average total site visits per month **	3,500,000	<5,000	11,664
IR1.6	Peak site visits per day **	155,000	<1,000	892
IR1.7	Average Page Impressions per month **	4.8 mil	<20,000	98,928
IR1.8	Number of unique editors	6	2	1
IR1.9	Average Search Requests per month **	750,000	N/A	N/A
IR1.10	CDN traffic requirement per month **	1.1 TB	N/A	N/A
IR1.11	Backup tape storage requirement per month **	1 TB	10GB	1 TB
IR1.12	Number of Provider Portal user accounts activated (total)***	N/A	N/A	7,000 (10,000, 250,000)
IR1.13	Number of Provider Portal online transactions per month****	N/A	N/A	2,000 (4,000, 40,000)

* on 15 July 2015

** For April/May/June 2015

*** Provider Portal accounts are currently being rolled out to all sectors. The first figure is for number of accounts at the end of June 2015. The second figure is an estimate of the number of accounts expected by 31 December 2015 and the third figure is the maximum currently anticipated.

**** Monthly online transaction. The first figure is for June 2015, the second is an estimate for December 2015 and the third figure is the likely maximum number of transactions.

Schedule 2
Service Levels

Service Levels

Availability metric	Monthly target
Live environments and data -the service utilised by an End User, i.e. citizen or a business including all data	99.95%
Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%
Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%
Non-Live environments to be available during standard business hours	99%
Non-Live environments to be available outside standard business hours	95%
In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours	100%

Level	Description	Supplier will respond to Issue raised and commence investigation	Resolution targets	SLA monthly Target
Severity 1	an issue that results in the loss of a facility or function material to the proper operation of the systems	Usually immediate with a call back	Within 1 hour(s) of investigation commencing **	100%
Severity 2	an issue that results in loss or interrupted provision of a system, but does not prevent the Customer from carrying out his business	2 hours	Within 5 hours of investigation commencing	100%
Severity 3	an issue that affects a small number of users but does not prevent business critical activity	5 hours	Within 2 business days of investigation commencing	95%
Severity 4	an issue that affects how users perform tasks but workarounds are available	5 hours	Within 5 business days of investigation commencing	95%
Root cause of Severity 1 issues are to be provided in a report within 24 hours with recommendations for action to reduce the risk of reoccurrence				100%
All incidents (including Sev 3 and 4) resolved or closed (and corresponding problem record created) within 20 business days				100%

** For each separate Severity 1 issue that is not resolved in accordance with the SLA terms and conditions, and is proven to be caused by a failure in Axis12 meeting its hosting obligations, a credit to the value of 5% of the monthly hosting fee will be added to the client's account, such that the maximum credit in any one month that shall not exceed the monthly hosting fee.

Schedule 3
Charges

Service month	Support cost (ex VAT)	Hosting cost (ex VAT)	Licences (ex VAT)
November 2017			
December 2017			
January 2018			
February 2018			
March 2018			
April 2018			
May 2018			
June 2018			
July 2018			
August 2018			
September 2018			
October 2018			
November 2018			
December 2018			
January 2019			
February 2019			
March 2019			
April 2019			
May 2019			
June 2019			
July 2019			
August 2019			
September 2019			
October 2019			
Total			

- Support prices are based on [REDACTED] with an allocation of 10 days per month minimum
- Unused time from each month cannot be rolled over to subsequent months.
- 10 days per month is fixed for the first 12-month term.
- The number of days required for the second 12 month term can be amended but must be requested in writing 30 days prior to the start of the second term.
- If additional support time is required beyond the bulk time allocated for each month or if support time is required outside of a signed contract agreement, this will be billed at our non-contracted adHoc day rate [REDACTED] hosting provision that is required outside of a signed contract agreement (i.e. non-contracted hosting services) is subject to a 200% uplift of the costs shown above.
- Changes to the hosting platform can be instructed throughout the contract duration and may result in a cost increase or decrease proportionate to the increases/decreases being made.
- Offboarding, service transfer, knowledge transfer, and documentation activities will all incur costs, that will; be agreed at the time of instruction

Part B – Invoicing and Payment

1 Purpose of Part B

- 1.1 This part of the schedule sets out the method by which the Contractor shall raise invoices to the Customer for payment, together with the requirements which apply to such invoices, and the payment terms thereof.
- 1.2 The Contractor shall be entitled to raise an invoice in respect of any payment which falls payable to the Contractor pursuant to the Contract provided that each invoice is delivered to the Customer within 5 Working Days after:
 - (a) In respect of Monthly Service Charges, the end of the calendar month to which the relevant Monthly Service Charge relates; and
 - (b) In respect of Time and Materials Charges, the end of the month in respect of Time and Materials Charges consumed in that month.
- 1.3 In any event, all invoices must be provided to the Customer within six (6) months of completion of delivery of the relevant Services to which the invoice relates. Invoices delivered after expiry of this period shall be invalid and the Customer shall have no liability in respect of such invoices.
- 1.4 The Contractor shall invoice the Customer in respect of Services in accordance with the timescales specified for issue of invoices for the Charges as detailed in Part A of this schedule.
- 1.5 The Contractor shall ensure that each invoice contains the following information:
 - (a) the date of the invoice;
 - (b) a unique invoice number;
 - (c) the month or other period(s) to which the relevant Charges relate;
 - (d) the reference number of the purchase order issued by the Customer to which it relates (if any);

- (e) the dates between which the Services subject of each of the Charges detailed on the invoice were performed;
 - (f) details of any Service Credits or similar deductions that shall apply to the Charges detailed on the invoice;
 - (g) a contact name and telephone number of a responsible person in the Contractor's finance department in the event of administrative queries; and
 - (h) the banking details for payment to the Contractor via electronic transfer of funds (such as name and address of bank, sort code, account name and number).
- 1.6 Each invoice shall at all times be accompanied by sufficient information to enable the Customer to reasonably assess whether the Charges detailed thereon are properly payable. Any such assessment by the Customer shall not be conclusive. The Contractor undertakes to provide to the Customer any other documentation reasonably required by the Customer from time to time to substantiate an invoice.
- 1.7 All Contractor invoices shall be expressed in pounds sterling or such other currency as shall be permitted by the Customer in writing.
- 1.8 The Customer shall only regard an invoice as valid if it complies with the provisions of this schedule. Where any invoice does not conform to the Customer's requirements set out in this schedule, the Customer will return the disputed invoice to the Contractor. The Contractor shall promptly issue a replacement invoice which shall comply with the requirements of this Schedule.

Schedule 4

Governance

1 Governance Framework

1.1 The Contractor and the Customer shall operate a governance framework comprising the following;

- (a) Monthly Service Review meeting
- (b) Quarterly Contract Review meeting
- (c) Extraordinary meetings as necessary and requested by Customer

2 Monthly Service Review meeting

2.1 The Monthly Service Review meeting is a formal meeting between Customer and Contractor Service Managers to review service performance as measured against the contract. Minutes will be taken and actions recorded.

2.2 Attendees: Customer and Contractor Service Managers, others as required and invited.

2.3 Purpose: To review the Monthly Service Report detailing the delivered service performance as measured against the contract service levels; to review and agree work to address any on-going performance issues; and to review and agree continual service improvement activity.

3 Quarterly Service Review meeting

3.1 The Quarterly Contract Review meeting is a more strategic meeting between the Customer and Contractor Heads of Department. It will review and discuss contractual and commercial performance against the contract. Minutes will be taken and actions recorded.

3.2 Attendees: Customer and Contractor Heads of Department and Service Managers.

3.3 Purpose: To review the contractual and commercial health of the relationship; to discuss areas for business development and improvement.

4 Extraordinary meetings

4.1 Extraordinary meetings will occur as necessary. Meetings arranged, possibly a short notice to address urgent and/or high impact issues or incidents.

4.2 Attendees: Customer and Contractor representatives as appropriate.

4.3 Purpose: To address and agree action in response to extraordinary events whether technical, contractual or external to CRM that either already have, or have the potential to, impact service performance and delivery.

5 Continual Service Improvement

5.1 The Contractor and the Customer will carry out continual service improvement (CSI) to regularly capture, review and execute measures that improve the quality, performance, usability and relevance of Seibel CRM during the Contract Period.

- 5.2 The Contractor and the Customer will maintain a CSI Register to capture and record potential opportunities to improve the service. CSI items and suggestions can be added to the CSI Register at any time by any Customer or Contractor representative.
- 5.3 As part of the Monthly Service Review, the Contractor and the Customer shall review the CSI Register and agree new CSI activities that will be carried out as well as review progress of CSI activities that are already in progress.

Schedule 5

Exit Management

1 Overview

- 1.1 The Contractor is required to ensure the orderly transition of the Services from the Contractor to the Customer and/or any replacement supplier in the event of termination or expiry of this Contract. This schedule sets out the principles of the exit and service transfer arrangements that are intended to achieve such orderly transition and which shall form the basis of the Exit Plan. For the avoidance of doubt, the Contractor shall be responsible for the overall management of the exit and service transfer arrangements.
- 1.2 The Contractor, at the Customer's expense, shall carry out the necessary activities to transfer responsibility for the delivery of the Services to the Customer and/or a new service provider (as required by the Customer) upon the earlier of the following:
- (a) expiry of this Contract on the Expiry Date; or
 - (b) termination of this Contract in accordance with this Contract and/or the Framework Agreement.
- 1.3 This Schedule defines the scope of an Exit Plan and how such a plan will be created and revised to ensure that it remains workable at any time upon termination or expiry. Where only the principles of such Exit Plan are set out then the parties will reach agreement on detailed terms and conditions in respect of such principles and such agreement shall not be unreasonably delayed or withheld.

2 Exit Plan

- 2.1 The Contractor shall, with input as relevant, from the Customer, create within 3 months of the Commencement Date an Exit Plan which envisages the requirements in relation to an exit of the Services covered by this Contract.
- 2.2 The Customer shall review the content of the Exit Plan submitted to it by the Contractor in accordance with paragraph 2.1 above and the Customer and the Contractor shall, acting reasonably and in good faith, seek to agree the contents of the Exit Plan within 30 days of submission of the same by the Contractor under paragraph 2.1. Should the Customer and the Contractor be unable to reach agreement, the matter will be referred to the Dispute Resolution Process.
- 2.3 The Contractor shall review the Exit Plan with the Customer periodically during the Term, as a minimum once every 6 months, and shall update it in order to reflect and take account of any Changes to the Services and/or their method of delivery.

3 Scope of Exit Plan

- 3.1 The Exit Plan shall contain:
- (a) a list and timetable of activities for the Contractor and the Customer to undertake during the Termination Assistance Period in sufficient detail to ensure that each party can comply with the terms of this Schedule 7 and to allow the smooth transition of the Services to any replacement supplier(s) with no disruption to the business of the Customer;
 - (b) details of which Contractor activities shall be provided free of charge (which shall include returning to the Customer all Specifically Created Material and all Customer Material to the Customer), and which activities shall be chargeable in accordance with paragraph 7 below;

- (c) full details of dependencies on the Customer and on the Contractor for the successful implementation of the Exit Plan;
- (d) such other details as the Customer and the Contractor consider appropriate when agreeing the terms of the Exit Plan; and
- (e) without prejudice to paragraph 8, the Termination Assistance that the Contractor will reasonably be required to provide to the Customer.

3.2 During any period when the Exit Plan has not been agreed by the Customer and the Contractor, the Exit Plan shall be deemed to be, and the Customer and the Contractor shall comply with, the terms detailed in this Schedule.

4 Notification of Requirements for Termination Assistance

4.1 The Customer shall have the right to require the provision of Termination Assistance by giving written notice to the Contractor at least one month prior to the Expiry Date of this Contract or at any time following service of a notice of Termination (a "Termination Assistance Request"). The Termination Assistance Request shall specify:

- (a) the date from which Termination Assistance is required, provided that such date is no earlier than:
 - (i) in the case of Termination, a date which is 10 (ten) days from the date of service of the Termination Assistance Request; and
 - (ii) in the case of expiry only (and not earlier Termination), 1 (one) month prior to expiry (the "Activation Date");
- (b) the nature and extent of the Termination Assistance required in accordance with paragraph 8;
- (c) if not already provided, confirmation as to whether the Terminating Services are to be continued in accordance with paragraph 5; and
- (d) the period during which the Customer envisages that Termination Assistance will be required, provided that such period will continue no longer than 3 months after the date that the Contractor ceases to provide the Terminating Services (the "Deactivation Date").

4.2 The period between the Activation Date and Deactivation Date shall be the Termination Assistance Period.

4.3 For the sake of clarity, in this Schedule "Termination Assistance" excludes "Terminating Services"

5 Continuation of the Terminating Services

5.1 In the event of the early Termination or the expiry of this Contract (for whatever reason), the Contractor shall, and shall ensure that all of its subcontractors (if any) and staff shall, to the extent requested by the Customer, in addition to supplying any other Termination Assistance pursuant to this Schedule 7, continue to perform the Terminating Services for the period specified in the notice of Termination and/or the Termination Assistance Request, which period shall not exceed 3 months after either the date on which Termination becomes effective or the Expiry Date.

5.2 Where the Customer requires the Contractor to continue the provision of some or all of the Terminating Services, such Terminating Services shall be provided at no detriment to the applicable Service Levels.

6 Exit Management and the Implementation of the Exit Plan

- 6.1 The Customer and the Contractor shall each advise the other in writing within 10 (ten) Working Days of the Activation Date of the identity of its staff responsible for the management of the exit from the Contract (**the Exit Managers**).
- 6.2 The Exit Managers shall promptly review the Exit Plan, and shall determine whether any amendments to the Exit Plan are required and shall discuss any other issues or matters relevant to the provision of Termination Assistance by the Contractor in accordance with the Exit Plan and this Schedule.
- 6.3 Upon agreement of any amendments to the Exit Plan, or if no such amendments are required, immediately following such review, the Contractor shall commence the implementation of the Exit Plan.
- 6.4 In order to facilitate implementation of the Exit Plan, the Contractor shall maintain:
- (a) A list of all assets used in providing the Services (including those that are owned by the Contractor);
 - (b) such documentation as is necessary to detail the technical aspects of the Services. This documentation shall be of sufficient detail to permit the Customer and any replacement supplier of the Services to understand how the Contractor provides the Services and to enable the smooth transition of the Services with the minimum of disruption to the Customer;
 - (c) details of other relevant third party contracts; and

in each case, the Customer may audit such documentation prior to implementation of the Exit Plan. The Contractor shall provide to the Customer such information, documents and details promptly upon request by the Customer.

7 Costs

- 7.1 In respect of and for the duration of the continuance of the provision of the Terminating Services pursuant to paragraph 5, the Customer shall continue to pay the Charges in respect of the Terminating Services in accordance with Schedule 5 (Charges).
- 7.2 The Contractor shall be entitled to charge the Customer on a time and materials basis in accordance with Schedule 5 (Charges) for the provision of any Termination Assistance provided that:
- (a) the Contractor shall use reasonable endeavours to reallocate resources to provide any Termination Assistance without additional costs;
 - (b) where additional cost is incurred, the Contractor can demonstrate to the Customer that such charges are reasonable; and
 - (c) the scope of the Termination Assistance and estimated fees in respect of the same have been previously authorised by the Customer.

8 Termination Assistance

- 8.1 The Contractor shall fully co-operate with and assist the Customer and/or any replacement supplier(s) in ensuring the smooth handover and continued running of the Services during the Termination Assistance Period. In particular, the Contractor shall, and shall procure that its subcontractors (if any) shall, render all such assistance to the Customer and/or the replacement supplier(s) as the Customer may reasonably require including (but not limited to) the following:
- (a) implementing and complying with the Exit Plan;
 - (b) providing an inventory of application software and documentation;

incomplete MI Report within 5 UK working days following receipt of any such reminder.

45.11 If there are 2 or more MI Failures in any 3-month rolling period, the Authority charge the Contractor for the costs (an 'admin fee') of chasing the Contractor to provide the required information.

46. Transparency and Access to Records
Transparency

46.1 In accordance with the government's policy on transparency, the Authority reserves the right to make all or part of the information (including this Contract) publicly available (subject to any redactions made at the discretion of Authority by considering and applying relevant exemptions under the FoIA).

46.2 The terms of this Contract permit all of the following:

- the Authority to publish the full text of such Contract concluded with the Contractor
- the Authority to publish the Contract after considering (at the Authority's sole discretion) any representations made by the Contractor regarding the application of any relevant FoIA or EIR exemptions

46.3 Not used

Who can carry out an audit or inspection?

46.4 Representatives of the following auditors will have access to the Contractor's records and accounts:

- the Cabinet Office
- the Department for Health
- the Authority
- the National Audit Office
- any auditor appointed by the Audit Commission

What will happen during the Contract term?

46.5 The Contractor will keep and maintain in accordance with Good Industry Practice and generally accepted accounting principles, full and accurate records and accounts of all of the following:

- the operation of this Contract
- the Services provided under this Contract (including any subcontracts)
- the amounts paid by each Authority under the Contract.

What will happen when the Contract ends?

46.6 The Contractor will provide a completed self-audit certificate to the Authority within 3 months. A template certificate is provided in Annex 3.

46.7 The Contractor's records and accounts will be kept until the latest of the following dates:

- 7 years after the date of termination or expiry of this Contract.
- another date that may be agreed between the Parties

46.8 During the timeframes highlighted in clause 7.7, the Contractor will:

- allow the previously listed auditors to inspect or audit its records
- keep the data the Contracts
- keep commercial records of:
 - the Charges, and any variations to them (actual or proposed)
 - costs, including Subcontractors' costs
- keep books of accounts for this Contract
- keep MI reports
- maintain access to its published accounts and trading entity information
- maintain proof of its compliance with its obligations under the Data Protection Act and the Transparency provisions set out in this Clause 7
- maintain records of its delivery performance under each Contract, including that of Subcontractors

What will happen during an audit or inspection?

46.9 The auditor will use reasonable endeavours to ensure that the conduct of the audit does not:

- unreasonably disrupt the Contractor
- materially delay the provision of Services under the Contract

-
- 46.10 Subject to any Confidentiality obligations, the Contractor will use reasonable endeavours to:
- provide information without delay
 - provide all information within scope
 - give auditors access to:
 - all information requested by the Auditor within the scope of the audit
 - the Contractor's staff
- 46.11 An auditor will be able to review, inspect and examine the Contractor's records and accounts associated with this Contract. This is to:
- verify the accuracy of:
 - the Charges (and proposed or actual variations to them in accordance with this Contract)
 - review the integrity, Confidentiality and security of the Personal Data and Authority Data held or used by the Contractor
 - review any books of accounts kept by the Contractor in connection with the provision of the Services, for the purposes of auditing the Charges under the Contract
 - review any other aspect of the delivery of the Services including to review compliance with any legislation
 - verify the accuracy and completeness of any MI delivered or required by this Contract
 - review any MI Reports and/or other records relating to the Contractor's performance of the Services and to verify that these reflect the Contractor's own internal reports and records
 - inspect the Authority's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Authority's assets are secure and that any asset register is up to date

Costs of conducting audits or inspections

- 46.12 The Contractor will reimburse the Authority's reasonable costs incurred in relation to the audit or inspection, if it reveals that the Contractor has committed a material Default
- 46.13 Each Party is responsible for covering all other costs that they may incur from their compliance with the obligations of this Contract.

47. Relationship of the Parties

Neither Party can act as agent of the other or make representations on their behalf.

49. Freedom of Information Act

- 49.1 The Contractor acknowledges that the Authority is subject to the requirements of the Freedom of Information Act (FoIA) and the Environmental Information Regulation (EIR).
- 49.2 The Contractor will help and co-operate with the the Authority to enable them to comply with their Information disclosure obligations regarding this Contract
- 49.3 The Contractor will in no event respond directly to a Request for Information under the FoIA.
- 49.4 The Contractor will note that the Information disclosed in response to a FoIA or EIR request may include its response. This may include attachments, embedded documents, any score or details of the evaluation of a response.
- 49.5 If the Contractor considers any part of its response to be confidential or commercially sensitive, the Contractor will:
- identify this Information
 - explain the potential implications of its disclosure, specifically addressing the public interest test as in the FoIA
 - estimate how long it believes such Information will remain confidential or commercially sensitive

49.6 The Authority will then consider whether or not to withhold such Information from publication. Even where Information is identified as confidential or commercially sensitive, the Authority may be required to disclose such Information in accordance with the FoIA or the EIR.

49.7 The Authority must form an independent judgement of whether the Contractor's Information is exempt from disclosure under the FoIA or the EIR and whether the public interest favours disclosure or not. Contractors must refer any request for Information, including requests relating to the procurement, to the Authority.

50. Promoting tax compliance

50.1 If tax non-compliance occurs during the Contract the Contractor will:

- notify the Authority in writing within 5 UK working days of its occurrence
- promptly provide the Authority with:
 - details of the steps that the Contractor is taking to address the non-compliance
 - other information in relation to the non-compliance as the Authority may reasonably require

50.2 If the Contractor fails to comply with this clause or does not provide details of its proposed mitigating factors, which in the reasonable opinion of the Authority are acceptable, then the Authority reserves the right to terminate this Contract for material Default.

51. Official Secrets Act

The Contractor will comply with and ensure that the Contractor Staff comply with the provisions of the Official Secrets Act 1911 to 1989 and Section 182 of the Finance Act 1989.

52. Subcontracting

52.1 The Contractor will deliver the services offered themselves, and will not solely source staff for others.

52.2 The Contractor will only subcontract with the approval of the Authority. If the Contractor chooses to use Subcontractors, this will be outlined in to the Authority in writing along with the percentage of delivery allocated to each Subcontractor.

52.3 The Contractor will take direct contractual responsibility and full accountability for delivering the services they provide using Subcontractors.

53. Complaints handling and resolution

53.1 Either Party will notify the other Party of any complaints made by the Authority, which are not resolved within 5 UK working days.

53.2 If the Contractor is the Party providing the notice, the notice will contain full details of the Contractor's plans to resolve the complaint.

53.3 The Contractor will work to resolve the complaint within 10 UK working days.

53.4 Within 2 UK working days of a request by the Authority, the Contractor will provide full details of a complaint, including details of steps taken to resolve it.

54. Communication

54.1 Any notices sent in relation to this Contract must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'. The Authority's email address is: Procurement@cqc.org.uk

54.2 The following table sets out the method by which notices may be served under this Contract and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of delivery	Proof of Service
--------------------	-------------------------	------------------

Email	9am on the first Working Day after sending	Dispatched in an emailed pdf to the correct email address without any error message
-------	--	---

55. Severability

- 55.1 If any part of the Contract becomes invalid, illegal or unenforceable, it will be severed from the Contract and the remaining parts of the Contract will be unaffected.
- 55.2 If any fundamental part of this Contract becomes invalid, the Authority and the Contractor may agree to remedy the invalidity. If the Parties are not able to do so within 20 UK working days of becoming aware of the invalidity, the Contract will be automatically terminated and each Party will be responsible for their own costs arising from the termination of the Contract.

[END]

