Crown Commercial Service

ATTACHMENT 4

Framework Agreement

CROWN COMMERCIAL SERVICE

and

Axis12 Ltd

RM 1557vi

G-CLOUD SERVICES 6

FRAMEWORK AGREEMENT

Contents

THIS AGREEMENT is made on 11 April2016

BETWEEN:

(1) THE MINISTER FOR THE CABINET OFFICE acting through Crown Commercial Service, part of the Crown, of 9th Floor, The Capital, Old Hall Street, Liverpool, L3 9PP (hereinafter called the "**Authority**"), and

(2) Axis12 Ltd, a company registered in England under company number 07215135 and whose registered office is at Unit 14, The Ivories, 6-18 Northampton Street, London, N1 2HY (the "**Supplier**").

NOW IT IS HEREBY AGREED as follows:

PART ONE: FRAMEWORK ARRANGEMENTS

FW-1 DEFINITIONS AND INTERPRETATION

FW-1.1 In this Framework Agreement expressions have the meaning ascribed in Framework Schedule 6 (Interpretations & Definitions) and this Framework Agreement shall be interpreted in accordance with the provisions of that Schedule.

FW-1.2 All eleven schedules annexed to this Framework Agreement Schedule 1: G-Cloud Services; Schedule 2: Call-Off Terms; Schedule 3: Call-Off Ordering Procedure; Schedule 4: Management Information Requirements; Schedule 5: Records and Audit Access and Schedule 6: Interpretations Definitions; Schedule 7: Collaboration Agreement; Schedule 8: Implementation Plan; Schedule 9: Alternative Clauses; Schedule 10a: Suppliers Solution for Digital Hosting, Schedule 10b: Suppliers Solution for Digital Hosting Managed Service and Schedule 11: Charges are expressly made a part of this Framework Agreement and are hereby made effective.

FW-2 SUPPLIER APPOINTMENT

FW-2.1 The Authority appoints the Supplier as the potential provider of G-Cloud Services and G-Cloud Additional Services in accordance with the terms of the Supplier's Tender and the Supplier shall be eligible to be considered for the award of orders for such G-Cloud Services and G-Cloud Additional Services by the Authority and Other Contracting Bodies during the Term; and in consideration of the Supplier agreeing to enter into this Framework Agreement and to perform its obligations under it the Authority agrees to pay and the Supplier agrees to accept on the signing of this Framework Agreement the sum of Five Pence (£0.05).

FW-3 TERM OF FRAMEWORK AGREEMENT

FW-3.1 This Framework Agreement shall take effect on (the "**Commencement Date**") and its term ("**Term**") shall expire twelve (12) Months after the Commencement Date, unless it is extended by the Authority at its sole discretion by written notice to the Supplier by one further period of six (6) Months and in either case unless it is terminated earlier in accordance with the terms of this Framework Agreement or otherwise by operation of Law.

FW-4 SCOPE OF FRAMEWORK AGREEMENT

FW-4.1 This Framework Agreement governs the overall relationship between the Authority and the Supplier in respect of the provision of the said G-Cloud Services by the Supplier to the Authority and to Other Contracting Bodies.

FW-4.2 The Authority and Other Contracting Bodies may, at their absolute discretion and from time to time during the Term, order G-Cloud Services from the Supplier in accordance with the Ordering Procedures and subject to the provisions of the Call-Off Agreement.

FW-4.3 The maximum duration of any Call-Off Agreement pursuant to this Framework Agreement is twenty four (24) Months.

No undertaking nor any form of statement, promise, representation or obligation shall be deemed to have been made by the Authority or any Other Contracting Body in respect of the total quantities or values of the said G-Cloud Services to be ordered by them pursuant to this Framework Agreement and the Supplier acknowledges and agrees that it has not entered into this Framework Agreement on the basis of any such undertaking, statement, promise or representation.

FW-5 ASSURANCE VERIFICATION

FW-5.1 The Supplier notes and accepts that a key element in the operation of the Framework Agreement is an Assurance verification process whereby the Authority, and other agents appointed by the Authority, verifies any or all claims made by the Supplier in their response to the Invitation to Tender, in their Catalogue entries, and in their Service Definitions. Assurance verification process forms an integral part of the qualification process for this Framework Agreement. Thereafter, Assurance verification will continue to verify that any Catalogue entries and related Service Definitions are an accurate reflection of the actual characteristics of the G-Cloud Service offering and that the Supplier continues to meet the essential qualification criteria established at the award of this Framework Agreement. Supplier's failure thereafter to maintain the appropriate level of Assurance verification (described at http://gcloud.civilservice.gov.uk/supplier-zone/assurance) will result in the suspension of either the Supplier or the particular service offering.

FW-6 CATALOGUE

FW-6.1 The Supplier undertakes from the Commencement Date to maintain the Catalogue in accordance with the terms of its Tender and thereafter to maintain and regularly update its Catalogue entries for all G-Cloud Services offered under this Framework Agreement.

FW-6.2 The Supplier acknowledges and agrees that the prices and other terms quoted in its Catalogue entries as part of its Tender submission cannot be increased or amended (as applicable) during the Term of this Framework Agreement. The Supplier agrees to bring the existence of its offering in the Catalogue to the attention of any Contracting Body that enquires of it in relation to G-Cloud Services.

FW-6.3 The Supplier acknowledges and agrees that its Catalogue entries, pricing and terms and conditions pertaining to the G-Cloud Services shall be publicly available via the Digital Marketplace.

FW-6.4 Subject to the Authority's Approval (that shall not be unreasonably withheld or delayed) the Supplier may vary, but not materially change, the Catalogue entry and/or Service Definitions in respect of all Orders placed thereafter. Subject to notifying the Authority in writing, the Supplier may also remove the Catalogue entries. Once the G-Cloud Services have been ordered by a Contracting Body, the Supplier hereby undertakes to maintain the Supplier Terms as at the time of the Order and for the duration of any Call-Off Agreement.

FW-6.5 The Supplier may reduce any of their prices stated in the Catalogue at any time.

FW-6.6 The pricing of Call-Off Agreements must be based on the prices stated in the Supplier's Catalogue entry.

FW-6.7 If the Authority or any Other Contracting Body decides to source G-Cloud Services and any G-Cloud Additional Services through this Framework then it will select the relevant Framework Suppliers and choose between them in accordance with the Framework Schedule 3 (Call-Off Ordering Procedure).

PART TWO: SUPPLIER'S GENERAL FRAMEWORK OBLIGATIONS

FW-7 WARRANTIES AND REPRESENTATIONS

FW-7.1 The Supplier warrants represents and undertakes to the Authority and each Other Contracting Body that:

FW-7.1.1 it has used and shall continue to use all reasonable endeavours to prevent the introduction, creation or propagation of any disruptive elements (including any virus, worms and/or Trojans, spyware or other malware) into systems providing services to data, software or Authority Confidential Information held in electronic form (owned by or under the control of, or used by the Authority or any other Contracting Body); and

FW-7.1.2 in entering into this Framework Agreement and any Call-Off Agreement it has not committed any Fraud; and

FW-7.1.3 it owns, has obtained, (or has made reasonable endeavours to do so) or shall obtain (or shall make reasonable endeavours to obtain) valid licences for all Intellectual Property Rights that are necessary to perform its obligations under this Framework Agreement and/or any Call-Off Agreement which may be entered into with the Authority or Other Contracting Bodies and shall maintain the same in full force and effect for the duration of the Term and the duration of any and all Call-Off Agreements entered into by it under the Framework.

FW-7.2 For the avoidance of doubt, the fact that any provision within this Framework Agreement is expressed as a warranty shall not preclude any right of termination the Authority may have in respect of breach of that provision by the Supplier.

PART THREE: SUPPLIER'S OBLIGATIONS

FW-8 PROVISION OF MANAGEMENT INFORMATION

FW-8.1 The Supplier shall, at no charge to the Authority, submit to the Authority complete and accurate Management Information in accordance with the provisions of the Framework Schedule 4 (Management Information Requirements) using the template made available from time to time by the Authority for that purpose (the current form of which template is included as Annex A to Framework Schedule 4).

FW-8.2 The Supplier grants the Authority a non-exclusive, transferable, perpetual, irrevocable, royalty free licence to use and to share with any Other Contracting Bodies and Relevant Person any Management Information supplied to the Authority for the Authority's normal operational activities including administering this Framework Agreement and Call-Off Agreements, monitoring public sector expenditure, identifying savings or potential savings and planning future procurement activity.

FW-8.3 In the event the Authority shares the Management Information, any Other Contracting Body receiving such information shall be informed of the sensitive nature of that information and shall be requested not to disclose it to any person who is not a Crown body or Other Contracting Body (unless required to do so by Law).

FW-9 MANAGEMENT CHARGE

FW-9.1 In consideration of the establishment and award of this Framework Agreement and the management and administration by the Authority of same, the Supplier shall pay to the Authority the Management Charge in accordance with Clause FW-9.2.

FW-9.2 The Authority shall be entitled to submit invoices to the Supplier in respect of the Management Charge due each Month based on the Management Information provided pursuant to Framework Schedule 4 (Management Information Requirements).

FW-9.3 The Supplier shall pay the amount stated in any invoice submitted under Clause FW-9.2 within thirty (30) calendar days of the date of issue of the invoice.

FW-9.4 The Management Charge shall apply to the full Charges as specified in each and every Order and shall not be varied as a result of any reduction in the Charges due to the application of any service credits and/or any other deductions made under any Call-Off Agreement.

FW-9.5 The Management Charge shall be exclusive of VAT. The Supplier shall pay the VAT on the Management Charge at the rate and in the manner prescribed by Law from time to time.

FW-9.6 Interest shall be payable on any late payments of the Management Charge under this Framework Agreement in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

FW-9.7 The Authority shall be entitled to submit invoices to the Supplier in respect of the Admin Fees as set out in paragraph S4-2 of Framework Schedule 4 (Management Information Requirements) of this Framework Agreement.

FW-10 CONTRACTING BODY SATISFACTION MONITORING

FW-10.1 The Authority may from time to time undertake (or procure the undertaking of) a Contracting Body satisfaction survey (**"Contracting Body Satisfaction Survey"**) the purpose of which shall include:

FW-10.1.1 assessing the level of satisfaction among Contracting Bodies with the supply of G-Cloud Services (including the way in which the G-Cloud Services are provided, performed and delivered) and, in particular, with the quality, efficiency and effectiveness of the supply of the G-Cloud Services;

FW-10.1.2 monitoring the compliance by the Supplier with the terms of its Tender and its Catalogue entries; and

FW-10.1.3 such other assessment as it may deem appropriate for monitoring Contracting Body satisfaction.

FW-10.2 The Authority shall be entitled to include the results of Contracting Body Satisfaction Surveys in the Catalogue of G-Cloud Services and any Other Contracting Body shall be entitled, but not obliged, to use those results to make decisions under or in relation to this Framework Agreement, the Call-Off Agreements and any other contract between the Contracting Body and the Supplier.

FW-11 PUBLICITY AND BRANDING

FW-11.1 The Supplier shall at all times during the Term on written demand indemnify the Authority and keep the Authority fully indemnified against all losses, incurred by, awarded against or agreed to be paid by the Supplier arising out of any claim or infringement or alleged infringement (including the defence of such infringement or alleged infringement) resulting from the Supplier's use of the Authority's logo.

PART FOUR: TERMINATION AND SUSPENSION

FW-12 TERMINATION AND SUSPENSION OF SUPPLIER'S APPOINTMENT

FW-12.1 Any Supplier failure to comply with the obligations of this Framework Agreement, may lead to this Framework being terminated or suspended.

FW-12.2 The Authority may terminate or suspend this Framework Agreement at will by serving notice on the Supplier in writing with effect from the date specified in such notice.

FW-13 CONSEQUENCES OF SUSPENSION, TERMINATION AND EXPIRY

FW-13.1 Suspension from this Framework Agreement will not affect existing Call-Off Agreements. The Contracting Bodies concerned with such existing Call-Off Agreements will make their own decisions on whether to suspend or terminate those Call-Off Agreements and suspension or termination in those circumstances will be governed by the terms and conditions of the relevant Call-Off Agreements.

FW-13.2 Notwithstanding the service of a notice to terminate this Framework Agreement, the Supplier shall continue to fulfil its obligations under this Framework Agreement until the date of expiry of any Call-Off Agreement established under this Framework Agreement.

FW-13.3 Termination or expiry of this Framework Agreement shall not cause any Call-Off Agreements to terminate automatically. For the avoidance of doubt, all Call-Off Agreements shall remain in force unless and until they are terminated or expire in accordance with the terms of the Call-Off Agreement, and the Supplier shall continue to provide Management Information and to pay Management Charges due to the Authority in relation to such Call-Off Agreements, notwithstanding the termination or expiry of this Framework Agreement.

FW-13.4 Termination or expiry of this Framework Agreement shall be without prejudice to any rights, remedies or obligations of either the Authority or the Supplier accrued under this Framework Agreement prior to its termination or expiry.

PART FIVE: GENERAL PROVISIONS

FW-14 DISPUTE RESOLUTION

FW-14.1 The Authority and the Supplier shall attempt in good faith to negotiate a settlement of any dispute between them arising out of or in connection with this Framework Agreement within twenty (20) Working Days of either party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the Authority Representative and the Supplier Representative.

FW-14.2 If the dispute cannot be resolved by the Parties pursuant to Clause FW-14.1, the Parties shall refer it to mediation unless the Authority considers that the dispute is not suitable for resolution by mediation.

FW-14.3 If the dispute cannot be resolved by mediation the Parties may refer it to arbitration.

FW-14.4 The obligations of the Parties under this Framework Agreement shall not be suspended, cease or be delayed by the reference of a dispute to mediation or arbitration pursuant to this Clause FW-14 and the Supplier and Supplier's Staff shall continue to comply fully with the requirements of this Framework Agreement at all times.

FW-15 LAW AND JURISDICTION

FW-15.1 This Framework Agreement and/or any non-contractual obligations or matters arising out of or in connection with it, shall be governed by and construed in accordance with the Laws of England and Wales and without prejudice to the dispute resolution procedure set out in Clause FW-14 (Dispute Resolution) each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

FW-16 SEVERABILITY

FW-16.1 If any provision of this Framework Agreement is held invalid, illegal or unenforceable for any reason, such provision shall be severed and the remainder of the provisions hereof shall continue in full force without affecting the remaining provisions of this Framework Agreement.

FW-16.2 If any provision of this Framework Agreement that is fundamental to the accomplishment of the purpose of this Framework Agreement is held to any extent to be invalid,

the Authority and the Supplier shall immediately commence good faith negotiations to remedy such invalidity.

FW-17 WAIVER AND CUMULATIVE REMEDIES

FW-17.1 The rights and remedies provided by this Framework Agreement may be waived only in writing by the Authority Representative or the Supplier Representative in a manner that expressly states that a waiver is intended, and such waiver shall only be operative with regard to the specific circumstances referred to.

FW-17.2 Unless a right or remedy of the Authority is expressed to be an exclusive right or remedy, the exercise of it by the Authority is without prejudice to the Authority's other rights and remedies. Any failure to exercise or any delay in exercising a right or remedy by either Party shall not constitute a waiver of that right or remedy or of any other rights or remedies.

FW-17.3 The rights and remedies provided by this Framework Agreement are cumulative and, unless otherwise provided in this Framework Agreement, are not exclusive of any right or remedies provided at Law or in equity or otherwise under this Framework Agreement.

FW-18 RELATIONSHIP OF THE PARTIES

FW-18.1 Nothing in this Framework Agreement is intended to create a partnership, or legal relationship of any kind that would impose liability upon one Party for the act or failure to act of the other Party, or to authorise either Party to act as agent for the other Party. Neither Party shall have authority to make representations, act in the name of, or on behalf of, or to otherwise bind the other Party.

FW-19 LIABILITY

FW-19.1 Neither Party excludes or limits its liability for:

FW-19.1.1 death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors;

FW-19.1.2 bribery, Fraud or fraudulent misrepresentation by it or its employees; or

FW-19.1.3 breach of any obligations implied by section 2 of the Supply of Goods & Services Act 1982.

FW-19.2 The Supplier's liability in relation to the obligation to pay any Management Charges which are properly due and payable to the Authority shall not be limited.

FW-19.3 Subject to Clause FW-19.1 each Party's total aggregate liability in connection with this Framework Agreement (whether expressed as an indemnity or otherwise) in each twelve (12) Month period during the Term (whether in contract, tort (including negligence), breach of statutory duty or howsoever arising) shall be limited to a sum equivalent to one hundred and twenty five per cent (125%) of the Management Charge paid and payable in the Year of this Framework Agreement during which the default occurred. For the avoidance of doubt, the Parties acknowledge and agree that this Clause FW-19 shall not limit Supplier's and Other Contracting Bodies' liability under any Call-Off Agreement and that Supplier's and Contracting Bodies' liability in relation to a Call-Off Agreement shall be as set out in the Call-Off Agreement.

FW-19.4 Subject to Clauses FW-19.1 and FW-19.5, in no event shall either Party be liable to the other for any:

FW-19.4.1 loss of profits;

FW-19.4.2 loss of business;

FW-19.4.3 loss of revenue;

FW-19.4.4 loss of or damage to goodwill;

FW-19.4.5 loss of savings (whether anticipated or otherwise); and/or

FW-19.4.6 any indirect, special or consequential loss or damage.

FW-19.5 Subject to Clause FW-19.3 the Supplier shall be liable for the following types of loss, damage, cost or expense which shall be regarded as direct and shall (without in any way, limiting other categories of loss, damage, cost or expense which may be recoverable by the Authority) be recoverable by the Authority:

FW-19.5.1 any regulatory losses or fines arising directly from a breach by the Supplier of any Laws; and

FW-19.5.2 subject to Clause FW-19.1 any additional operational and/or administrative costs and expenses arising from any Material Breach.

FW-20 ENTIRE AGREEMENT

FW-20.1 Without prejudice to the foregoing, this Framework Agreement, together with a completed, signed and dated Call-Off Agreement and the other documents referred to in them constitute the entire agreement and understanding between the Parties in respect of the matters dealt with in it and supersedes, cancels or nullifies any previous agreement between the Parties in relation to such matters.

FW-20.2 Each of the Parties acknowledges and agrees that in entering into this Framework Agreement it does not rely on, and shall have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Framework Agreement.

FW-20.3 Nothing in this Clause shall operate to exclude liability or remedy for Fraud or fraudulent misrepresentation.

FW-21 NOTICES

FW-21.1 Any notices given under or in relation to this Framework Agreement shall be in writing by letter, signed by or on behalf of the Party giving it, sent by recorded delivery service and for the attention of the relevant Party set out in Clause FW-21.4 or to such other address as that Party may have stipulated in accordance with Clause FW-21.5.

FW-21.2 A notice shall be deemed to have been received two (2) Working Days from the date of posting.

FW-21.3 In proving service, it shall be sufficient to prove that the envelope containing the notice was addressed to the relevant Party set out in Clause FW-21.4 (or as otherwise notified by that Party) and delivered either to that address or into the custody of the postal authorities as recorded delivery.

FW-21.4 The address, fax number and e-mail address of each Party shall be:

FW-21.4.1 for the Authority:

Crown Commercial Service

Rosebery Court

St Andrews Business Park

Norwich

NR7 0HS

For the attention of: Suzanne Williams

Tel: 0345 410 2222

Email: info@ccs.gsi.gov.uk; and

FW-21.4.2 for the Supplier:

For the attention of: Luke Harrop

Tel: 0845 519 5465

Email: luke.harrop@axistwelve.com

FW-21.5 Either Party may change its address for service by serving a notice in accordance with this Clause.

FW-21.6 For the avoidance of doubt, any notice given under this Framework Agreement shall not be validly served if sent by electronic mail and not confirmed by a letter.

FW-22 PREVENTION OF BRIBERY AND CORRUPTION

FW-22.1 If the Supplier breaches the Bribery Act 2010 in relation to this Framework Agreement, the Authority may terminate this Framework Agreement.

FW-22.2 The Parties agree that the Management Charge payable in accordance with Clause FW-9 does not constitute an offence under section 1 of the Bribery Act 2010.

FW-23 SAFEGUARDING AGAINST FRAUD

FW-23.1 The Supplier shall notify the Authority immediately and in writing if it has reasons to suspect that any Fraud has occurred, is occurring or is likely to occur save where complying with this provision would cause the Supplier or its employees to commit an offence under the Proceeds of Crime Act 2002 or the Terrorism Act 2000.

FW-24 DATA PROTECTION AND DISCLOSURE

FW-24.1 The provisions of this Clause FW-24 shall apply during the Term and for such time as the Supplier holds the Authority Personal Data.

FW-24.2 The Supplier shall (and shall procure that Supplier's Staff) comply with any notification requirements under the DPA and both Parties undertake to duly observe all their obligations under the DPA which arise in connection with this Framework Agreement.

FW-24.3 Where the Supplier is Processing Authority Personal Data for the Authority the Supplier shall ensure that it has in place appropriate technical and organisational measures to ensure the security of the Authority Personal Data (and to guard against unauthorised or unlawful Processing of the Authority Personal Data and against accidental loss or destruction of, or damage to, the Authority Personal Data) and:

FW-24.3.1 provide the Authority with such information as the Authority may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;

FW-24.3.2 promptly notify the Authority of any breach of the security measures to be put in place pursuant to this Clause; and

FW-24.3.3 ensure that it does not knowingly or negligently do or omit to do anything which places the Authority in breach of its obligations under the DPA.

FW-24.4 The Supplier shall:

FW-24.4.1 not cause or permit to be Processed, stored, accessed or otherwise transferred outside the European Economic Area any Authority Personal Data supplied to it by the Authority without the prior Approval of the Authority and, where the Authority consents to such processing, storing, accessing or transfer outside the European Economic Area, to comply with:

FW-24.4.1.1 the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Authority Personal Data that is so Processed, stored, accessed or transferred;

FW-24.4.1.2 any reasonable instructions notified to it by the Authority or Contracting Body concerned; or,

FW-24.4.1.3 either incorporate standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) or warrant that that the obligations set out in the Supplier Terms provide Adequate protection for Personal Data.

FW-25 FREEDOM OF INFORMATION

FW-25.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and co-operate with the Authority to enable the Authority to comply with its Information disclosure obligations.

FW-25.2 The Supplier shall:

FW-25.2.1 transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receiving a Request for Information; and

FW-25.2.2 provide all necessary assistance reasonably requested by the Authority to enable the Authority to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

FW-25.3 The Authority shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Framework Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

FW-25.4 In no event shall the Supplier respond directly to a Request for Information unless expressly authorised to do so by the Authority.

FW-25.5 The Supplier acknowledges that (notwithstanding the provisions of this Clause FW-25) the Authority may, acting in accordance with the Ministry of Justice Code, be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Supplier or the G-Cloud Services:

FW-25.5.1 in certain circumstances without consulting the Supplier; or

FW-25.5.2 following consultation with the Supplier and having taken its views into account;

provided always that where Clause FW-25.5.1 applies the Authority shall, in accordance with any recommendations of the Ministry of Justice Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

FW-25.6 The Supplier acknowledges that the description of information as Commercially Sensitive Information in Framework Schedule 6 (Interpretation and Definitions) is of an indicative nature only and that the Authority may be obliged to disclose it in accordance with Clause FW-25.

FW-26 CONFIDENTIALITY

FW-26.1 Except to the extent set out in this Clause or where disclosure is expressly permitted elsewhere in this Framework Agreement, each Party shall:

FW-26.1.1 treat all Confidential Information belonging to the other Party as confidential and safeguard it accordingly; and

FW-26.1.2 not disclose any Confidential Information belonging to the other Party to any other person without the prior written approval of the other Party, except to such persons and to such extent as may be necessary for the performance of this Framework Agreement or is a requirement of Law.

FW-26.2 The Supplier shall take all necessary precautions to ensure that all Authority Confidential Information obtained under or in connection with this Framework Agreement:

FW-26.2.1 is given only to the Supplier Staff engaged to advise it in connection with this Framework Agreement as is strictly necessary for the performance of this Framework Agreement; and

FW-26.2.2 is treated as confidential and not disclosed (without Approval) or used by any Supplier Staff otherwise than for the purposes of and in accordance with this Framework Agreement.

FW-26.3 The Supplier shall ensure that the Supplier Staff are aware of the Supplier's confidentiality obligations under this Framework Agreement and shall use its best endeavours to ensure that the Supplier Staff comply with the Supplier's confidentiality obligations under this Framework Agreement and in relation to the Call-Off Agreements.

FW-26.4 The provisions of Clauses FW-26.1 to Clause FW-26.3 shall not apply to any Confidential Information received by one Party from the other which:

FW-26.4.1 is or becomes public knowledge (otherwise than by breach of this Clause FW-26);

FW-26.4.2 was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

FW-26.4.3 is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure;

FW-26.4.4 is information independently developed without access to the Confidential Information;

FW-26.4.5 must be disclosed pursuant to a statutory, legal or parliamentary obligation placed upon the Party making the disclosure, including any requirements for disclosure under Clause FW-27 (Transparency) and/or the FOIA, or the Environmental Information Regulations pursuant to Clause FW-25 (Freedom of Information); or

FW-26.4.6 is used for the purpose of obtaining professional advice.

FW-26.5 Nothing in this Framework Agreement shall prevent the Authority from disclosing the Supplier's Confidential Information (including the Management Information obtained under Clause FW-8):

FW-26.5.1 for the purpose of the examination and certification of the Authority's accounts;

FW-26.5.2 for the purpose of any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

FW-26.5.3 to any government department or any Other Contracting Body and the Supplier hereby acknowledges that all government departments or Contracting Bodies receiving such Supplier's Confidential Information may further disclose the Supplier's Confidential Information to other government departments or Other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any government department or any Contracting Body; or

FW-26.5.4 for the purpose of disseminating knowledge of the G-Cloud Services and their respective performance to Other Contracting Bodies.

FW-26.6 The Supplier acknowledges and agrees that for the purpose of ensuring consistent behaviour between the Customers and Suppliers to this Framework, information relating to Orders placed by a Contracting Body, including pricing information and the terms of any Call-Off Agreement:

FW-26.6.1 may be published by the Authority, subject to this Clause FW-26; and

FW-26.6.2 may be shared with Other Contracting Bodies from time to time. Where such information is shared with Other Contracting Bodies, the Authority shall notify the recipient of such information that its contents are confidential.

FW-26.7 In the event that the Supplier fails to comply with Clauses FW-26.1 to Clause FW-26.4, the Authority reserves the right to terminate this Framework Agreement with immediate effect by notice in writing.

FW-26.8 The Supplier will immediately notify the Authority of any breach of security in relation to Authority Confidential Information obtained in the performance of this Framework Agreement and the Call-Off Agreements and will keep a record of such breaches. The Supplier will use its best endeavours to recover such Authority Confidential Information however it may be recorded. This obligation is in addition to the Supplier's obligations under Clauses FW-26.1 to Clause FW-26.6. The Supplier will co-operate with the Authority in any investigation that the Authority considers necessary to undertake as a result of any breach of security in relation to Authority Confidential Information.

FW-27 TRANSPARENCY

FW-27.1 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Framework Agreement is not Confidential Information. The Authority shall be responsible for determining in its absolute discretion whether any of the content of this Framework Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

FW-27.2 Notwithstanding any other term of this Framework Agreement, the Supplier hereby gives his consent for the Authority to publish this Framework Agreement in its entirety, (subject to any information that is exempt from disclosure in accordance with the provisions of FOIA redacted) including from time to time agreed changes to this Framework Agreement, to the general public.

FW-27.3 The Authority may consult with the Supplier to inform its decision regarding any FOIA exemptions under Clause FW-26 but the Authority shall have the final decision in its absolute discretion.

FW-27.4 The Supplier shall assist and cooperate with the Authority to enable the Authority to publish this Framework Agreement. It is the Authority's intention to publish Catalogue entries, Service Definitions, Supplier Catalogue prices, Supplier Terms as set out in Schedule 1 (G-Cloud

Services), Supplier's Assurance and accreditation verification results, performance feedback from Contracting Bodies Satisfaction Survey, Authority Management Information, and summary information relating to Orders including but not limited to Supplier, G-Cloud Services, Contracting Body, Order dates and Order value. It is not the Authority's intention to publish Supplier designs or processes, Supplier IPR or the details from accreditation supporting documentation.

FW-28 EQUALITY AND DIVERSITY

FW-28.1 The Supplier shall:

FW-28.1.1 perform its obligations under this Framework Agreement (including those in relation to the provision of the G-Cloud Services) in accordance with:

FW-28.1.1.1 all applicable equality Law (whether in relation to race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise); and

FW-28.1.1.2 any other requirements and instructions which the Authority and/or the Contracting Body reasonably imposes in connection with any equality obligations imposed on the Authority and/or the Contracting Body at any time under applicable equality Law.

FW-29 OFFICIAL SECRETS ACTS

FW-29.1 The Supplier shall (where applicable) comply with and shall ensure that the Supplier Staff comply with, the provisions of:

FW-29.1.1 the Official Secrets Act 1911 to 1989; and

FW-29.1.2 Section 182 of the Finance Act 1989.

FW-29.2 In the event that the Supplier or the Supplier Staff fail to comply with this Clause, the Authority reserves the right to terminate this Framework Agreement with immediate effect by giving notice in writing to the Supplier.

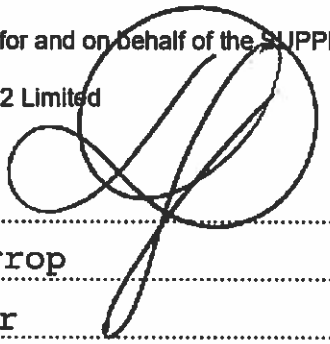
FW-30 THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

FW-30.1 A person who is not party to this Framework Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Framework Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

BY SIGNING AND RETURNING THIS FRAMEWORK AGREEMENT THE SUPPLIER AGREES to comply with all the terms of this legally binding Framework Agreement Ref: RM1557vi to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read this Framework Agreement and its Schedules and by signing below agree to be bound by the terms of this Framework Agreement.

Signed duly authorised for and on behalf of the SUPPLIER

Company Name: Axis 12 Limited



Signature: .....

Name: Luke Harrop

Position: Director

Date: 4.5.2016

Signed for and on behalf of the AUTHORITY

Name: Care Quality Commission

Signature: .....

Name: Sally Collier .....

Position: Managing Director .....

Date: .....

Schedule 1: G-Cloud Services

G-CLOUD SERVICES

S1-1 This Framework Agreement covers the provision of G-Cloud Services including but not limited to:

S1-1.1 LOT 1

S1-1.1.1 Infrastructure as a service (IaaS) as defined by the U.S. Department of Commerce, National Institute of Standards and Technology ("**NIST**") as:

> the capability provided to the Customer is to provision processing, storage, networks, and other fundamental computing resources where the Customer is able to deploy and run arbitrary software, which can include operating systems and applications. The Customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

S1-1.2 LOT 2

S1-1.2.1 Platform as a service (PaaS) as defined by NIST as:

> the capability provided to the Customer is to deploy onto the cloud infrastructure Customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the Supplier. The Customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

S1-1.3 LOT 3

S1-1.3.1 Software as a service (SaaS) as defined by NIST as:

> the capability provided to the Customer is to use the Supplier's applications running on a cloud infrastructure2. The applications are accessible from various Customer devices through either a thin Customer interface, such as a web browser (e.g., web-based email), or a program interface. The Customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

S1-1.4 LOT 4

S1-1.4.1 Specialist G-Cloud Services:

S1-1.4.1.1 Onboarding services for G-Cloud Services only

S1-1.4.1.2 Design Authority

S1-1.4.1.3 Business analysis for G-Cloud Services only

S1-1.4.1.4 Design and development

S1-1.4.1.5 Project specification and selection

S1-1.4.1.6 Deployment

S1-1.4.1.7 Transition management

S1-1.4.1.8 User management

S1-1.4.2 Service Integration and Management Services (SIAM):

S1-1.4.2.1 Enterprise architecture

S1-1.4.2.2 Project management and governance

S1-1.4.2.3 Service and systems integration

S1-1.4.2.4 Service management

S1-1.4.2.5 Software support

S1-1.4.2.6 Helpdesk

S1-1.4.3 Information management and digital continuity:

S1-1.4.3.1 eDiscovery

S1-1.4.3.2 Data recovery, conversion and migration

S1-1.4.3.3 Data quality

S1-1.4.3.4 Digital archiving

S1-1.4.3.5 Data storage consultancy for G-Cloud Services only

S1-2 G-CLOUD ADDITIONAL SERVICES

S1-2.1 The G-Cloud Additional Services are designed to be delivered as components of an integrated service model and are considered by the Authority to be enabling services to allow for an end to end delivery of the G-Cloud Services.

S1-2.2 A full service description for G-Cloud Additional Services must be included by the Supplier and the service MUST be G-Cloud Service related. In the event that the service is deemed not to be G-Cloud Services related they will be removed from the Framework.

S1-2.3 G-Cloud Additional Services are defined as ancillary services required to ensure the correct operation of the primary G-Cloud Services.

S1-2.4 For the avoidance of doubt, the following services are excluded from G-Cloud Additional Services:

a) Co-Location Services;

b) Non-Cloud related services/ consultancy;

c) Bespoke digital project build services for agile software development;

d) Hardware.

S1-3 SERVICE DEFINITION

S1-3.1 The Tender shall include a Service Definition for each service which shall include, but shall not be limited to the following headings:

S1-3.1.1 An overview of the G-Cloud Service (functional, non functional);

S1-3.1.2 Information assurance –

S1-3.1.2.1 Whether you hold a suitably scoped ISO27001 certificate for this G-Cloud Service.

S1-3.1.2.2 Relevant information surrounding your service in relation to the Government Security Classification (GSC) scheme

S1-3.1.3 Details of the level of data restoration/backup/restore and disaster recovery that will be provided;

S1-3.1.4 On-boarding and off-boarding processes/service migration/scope etc.;

S1-3.1.5 A brief overview of pricing (including unit prices, volume discounts (if any), data extraction etc.);

S1-3.1.6 Service management details;

S1-3.1.7 Service constraints (e.g. maintenance windows, level of customisation permitted, schedule for deprecation of functionality/features etc.);

S1-3.1.8 Service levels (e.g. performance, availability, support hours, severity definitions etc.);

S1-3.1.9 Financial recompense model for not meeting service levels;

S1-3.1.10 Training;

S1-3.1.11 Ordering and invoicing process;

S1-3.1.12 Termination process:

S1-3.1.12.1 By consumers (i.e. consumption); and

S1-3.1.12.2 By the Supplier (removal of the G-Cloud Service);

Technical requirements (service dependencies and detailed technical interfaces, e.g. client side requirements, bandwidth/latency requirements etc.) and details of any trial service available.

S1-3.2 The Supplier was successful in Lot(s):

Lot 2 and Lot 4

S1-4 THE SUPPLIER TERMS

S1-4.1 The Supplier Terms will be the terms and conditions set out in the form supplied as part of their Tender.

Schedule 2: Call-Off Terms

Date	26/01/2016	**Order Reference**	CQC ICTC 558 CQC ICTC 554

FROM:

Customer	Care Quality Commission **"Customer"**
Customer's Address	151 Buckingham Palace Road, London, SW1W 9SZ
Invoice Address	CARE QUALITY COMMISSION T70 PAYABLES F175 PHOENIX HOUSE TOPCLIFFE LANE WAKEFIELD WF3 1WE
Principal Contact	Name: Chris Day Address: 151 Buckingham Palace Road, London, SW1W 9SZ Phone: 020 7448 9307 e-mail:chris.day@cqc.org.uk

TO:

Supplier	Axis12 Ltd **"Supplier"**
Supplier's Address	Unit 14, The Ivories, 6-18 Northampton Street, London, N1 2HY
Account Manager	Name: Luke Harrop Address: Unit 14, The Ivories, 6-18 Northampton Street, London, N1 2HY Phone:0845 519 5465 e-mail: luke.harrop@axistwelve.com

1. TERM

1.1 Commencement Date

This Call-Off Agreement commences on: 26/01/2016

1.2 Expiry Date

This Call-Off Agreement shall expire on:

1.2.1 26/01/2017; or

1.2.2 the second (2) anniversary of the Commencement Date; whichever is the earlier, unless terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.

1.3 Services Requirements

1.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

1.3.2 G-Cloud Services

All Services as stipulated in Appendix A of the Clarification of understanding.

1.3.2.1 Lot1 IaaS	N/A;
1.3.2.2 Lot 2 PaaS	CQC Digital Hosting – see below
1.3.2.3 Lot 3 SaaS	N/A; and / or
1.3.2.4 Lot 4 Specialist G-Cloud Services	CQC Digital Hosting Managed Service – see below
1.3.2.5 G-Cloud Additional Services	N/A

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,10b and 10c 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,10b and 10c- 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 are 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 month **	1 TB	10GB	1 TB
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 service: a) CDN cache b) Page furniture cache (e.g. Nginx) c) 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	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

a 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 bespoking 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	Ability to SHH to all 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

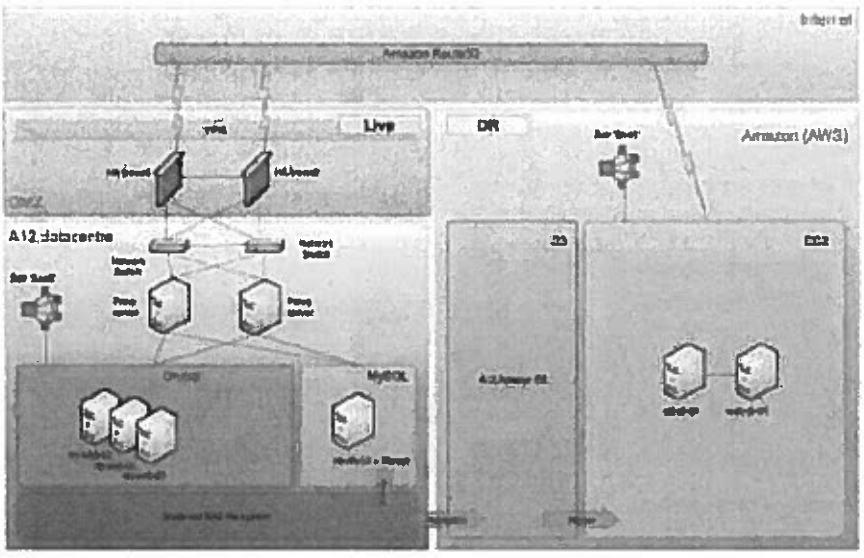
Community Sites

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	-

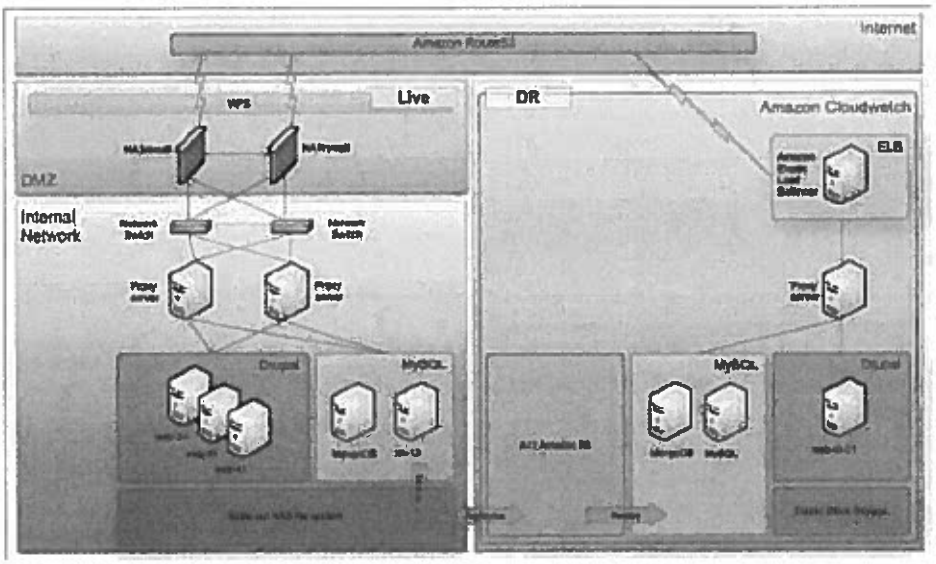
Provider Portal

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 Zenoss	N Y	N Y	N Y	Y Y	Y Y
IDS	Snort	N	N	N	N	N
Backups	Location Timing	- -	- -	- -	S3 00:00	- -
DNS	Management Owner	Route53 Axis12	Route53 Axis12	Route53 Axis12	Route53 Axis12	Route53 Axis12
URLs	Production (Live + DR)	https://services.cqc.org.uk http://authservices.axis12.com				
	Staging	https://stagingservices.cqc.org.uk				
	Test	https://test01services.cqc.org.uk https://test02services.cqc.org.uk				
	Dev	https://dev01services.axis12.com https://dev02services.axis12.com				
Disaster recovery	RPO RTO	- -	- -	- -	- -	24hrs 30mins
Tools	Jenkins New Relic	N N	N N	N N	N N	N N

System diagram



System Diagram - Provider



Lot 4- Specialist G-Cloud Services- 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 are 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 bespoking 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 and vs versa
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	Ability to SHH to all 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 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	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	Detail action points raised at major incident reviews and tracks them to resolution

	request	
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.

12 days per month will be provided to the supplier for ad-hoc support requests. Those days will have to 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	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 • 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	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 • 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	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
	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)
	Any fault in internal functionality of the Solution not visible to End Users (e.g. broken links report, enhanced feedback handling).
Visual	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 • 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	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
	One-off errors where functionality fails to comply with its agreed functional specification
	User queries 'How can I?' questions
Visual	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 • 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.*

2. PRINCIPAL LOCATIONS

2.1 Principal locations where the services are being performed

Services will be performed at Suppliers location, not CQC premises.

3. STANDARDS

3.1 Quality Standards

ISO 27001 certification for supplier and any hosting provider

All supplier staff to have current CRB checks

3.2 Technical Standards

No PSN requirements are needed

4. ONBOARDING

4.1 On-boarding

N/A

5. CUSTOMER RESPONSIBILITIES

5.1 Customer's Responsibilities

Customer Responsibilities as stipulated in Appendix A of Clarification of Understanding and the Framework terms.

5.2 Customer's equipment

CQC will provide licenses directly for EdgeCast CDN and Google APIs

6. PAYMENT

6.1 Payment profile and method of payment

Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS

The service will be paid by equal monthly payments in arrears.

Indicate preferred payment profile by selecting one from:

6.1.1 Monthly in arrears

6.2 Invoice format

The Supplier shall issue paper invoices Monthly in arrears. The Customer shall pay the Supplier within thirty (30) calendar days of receipt of a valid invoice, submitted in accordance with this paragraph 6.2, the payment profile set out in paragraph 6.1 above and the provisions of this Call-Off Agreement.

7. DISPUTE RESOLUTION

7.1 Level of Representative to whom disputes should be escalated to:

Simon Meredith – Head of Digital Development

7.2 Mediation Provider

Centre for Effective Dispute Resolution.

8. LIABILITY
Subject to the provisions of Clause CO 11 'Liability' of the Call–Off Agreement:
8.1 The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party (including technical infrastructure, assets, equipment or IPR but excluding any loss or damage to the Customer Data or Customer Personal Data) under or in connection with this Call–Off Agreement shall in no event exceed £.2,000,000 8.2 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall in no event exceed fifty percent (50%) of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period. 8.3 The annual aggregate liability under this Call–Off Agreement of either Party for all defaults shall in no event exceed the greater of £100,000 or one hundred and twenty five per cent (125%) per cent of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.

9. INSURANCE
9.1 Minimum Insurance Period Six (6) Years following the expiration or earlier termination of this Call-Off Agreement **9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:** - **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) 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 five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time.

10. TERMINATION
10.1 Undisputed Sums Time Period At least ninety (90) Working Days of the date of the written notice specified in Clause CO-9.4 of the Call-Off Agreement. **10.2 Termination Without Cause** At least thirty (30) Working Days in accordance with Clause CO-9.2 of the Call-Off Agreement.

11. AUDIT AND ACCESS
Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement.

12. PERFORMANCE OF THE SERVICES AND DELIVERABLES

12.1 Implementation Plan and Milestones (including dates for completion)

DN: Milestone table will be completed following successful supplier.

12.2 The Implementation Plan as at the Commencement Date is set out below

Milestone	Deliverables	Duration	Milestone Date	Customer Responsibilities
	Ability to copy databases from Production to non-Production environments and vice versa	0.5 day	22/02	
	Ability to download databases and assets to create local dev environments	0.5 day	23/02	
	Access to all code repositories and branches	0.5 days	24/02	
	Ability to deploy code to all environments	0.5 day	25/02	

12.2.1 If so required by the Customer, the Supplier shall produce within one (1) Month of the Commencement Date a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to Customer's written approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation transition and/or transformation of the G-Cloud Services.

12.2.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

12.2.3 The Supplier shall perform its obligations so as to achieve each milestone by the milestone date.

12.2.4 Changes to the milestones shall only be made in accordance with the Variation procedure as set out in Clause CO-21 and provided that the Supplier shall not attempt to postpone any of the milestones using the Variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a milestone by the relevant milestone date).]

12.3 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	99%

business hours	
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.

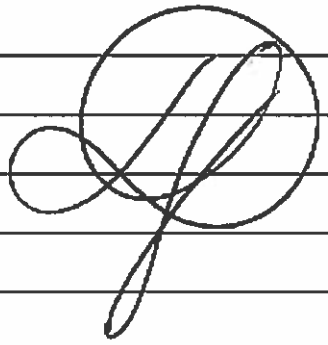
13. [COLLABORATION AGREEMENT
In accordance with Clause CO-20 of this Call-off Agreement, the Customer requires the Supplier to enter into

a Collaboration Agreement. The Collaboration Agreement shall be entered into on the Commencement Date.
11. [Alternative Clauses (select from Schedule 9: Alternative Clauses)]

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-Off Agreement.

For and on behalf of the Supplier:

Name and Title	Luke Harrop
Position	Director
Signature	
Date	4.5.2016



For and on behalf of the Customer:

Name and Title	EILEEN MILNER EXEC DIRECTOR
Position	EXEC DIRECTOR
Signature	Eileen Milner
Date	05.05.16.

G-CLOUD SERVICES CALL-OFF TERMS

Care Quality Commission

- and -

Axis12 Limited

relating to the provision of G-Cloud Services.

CALL-OFF AGREEMENT TERMS AND CONDITIONS

THIS CONTRACT is made on the [_26_] day of [_01_] 2016

BETWEEN

(1) Care Quality Commission of 151 Buckingham Palace Road, London, SW1W 9SZ [] (the "**Customer**"); and

(2) Axis12 Limited], a company registered in England under company number 07215135 and whose registered office is at Unit 14, 6-18 Northampton Street, London, N1 2HY (the "**Supplier**").

IT IS AGREED AS FOLLOWS:

CO-1 OVERRIDING PROVISIONS

CO-1.1 The Supplier agrees to supply the G-Cloud Services and any G-Cloud Additional Services in accordance with the Call-Off Terms, including Supplier's Terms as identified in Framework Schedule 1 (G-Cloud Services) and incorporated into this Call-Off Agreement.

CO-1.2 In the event of and only to the extent of any conflict or ambiguity between the Clauses of this Call-Off Agreement, the provisions of the Schedules, any document referred to in the Clauses of this Call-Off Agreement (including Supplier's Terms) and the Framework Agreement, the conflict shall be resolved in accordance with the following order of precedence:

CO-1.2.1 the Framework Agreement (excluding Framework Schedule 2);

CO-1.2.2 the Clauses of this Call-Off Agreement (excluding Supplier Terms);

CO-1.2.3 the completed Order Form;

CO-1.2.4 the Collaboration Agreement (Framework Schedule 7);

CO-1.2.5 the Supplier's Terms as set out in the Framework Schedule 1 (G-Cloud Services); and

CO-1.2.6 any other document referred to in the Clauses of this Call-Off Agreement.

CO-1.3 The Supplier acknowledges and accepts that the order of prevailing provisions in this Call-Off Agreement is as set out in Clause CO-1.2 above.

CO-2 PREVENTION OF BRIBERY AND CORRUPTION

CO-2.1 If the Supplier breaches

CO-2.1.1 Clauses FW-22.1 or FW-22.2 of the Framework Agreement; or,

CO-2.1.2 the Bribery Act 2010 in relation to the Framework Agreement

the Customer may terminate this Call-Off Agreement.

CO-2.2 The Parties agree that the Management Charge payable in accordance with Clause FW-9 does not constitute an offence under section 1 of the Bribery Act 2010.

CO-3 PROTECTION OF INFORMATION

CO-3.1 The provisions of this Clause CO-3, shall apply during the Call-Off Agreement Period and for such time as the Supplier holds the Customer Personal Data.

CO-3.2 The Supplier shall and shall procure that Supplier's Staff comply with any notification requirements under the DPA and both Parties undertake to duly observe all their obligations under the DPA which arise in connection with the Call-Off Agreement.

CO-3.3 To the extent that the Supplier is Processing the Order Personal Data the Supplier shall:

CO-3.3.1 ensure that it has in place appropriate technical and organisational measures to ensure the security of the Order Personal Data (and to guard against unauthorised or unlawful Processing of the Order Personal Data and against accidental loss or destruction of, or damage to, the Order Personal Data; and

CO-3.3.2 provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;

CO-3.3.3 promptly notify the Customer of any breach of the security measures to be put in place pursuant to this Clause; and

CO-3.3.4 ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of its obligations under the DPA.

CO-3.4 To the extent that the Supplier Processes Service Personal Data the Supplier shall:

CO-3.4.1 Process Service Personal Data only in accordance with written instructions from the Customer as set out in this Call-Off Agreement;

CO-3.4.2 Process the Service Personal Data only to the extent, and in such manner, as is necessary for the provision of the G-Cloud Services or as is required by Law or any Regulatory Body;

CO-3.4.3 implement appropriate technical and organisational measures to protect Service Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to Service Personal Data and having regard to the nature of the Service Personal Data which is to be protected;

CO-3.4.4 take reasonable steps to ensure the reliability of any Supplier Staff who have access to Service Personal Data;

CO-3.4.5 ensure that all Supplier Staff required to access Service Personal Data are informed of the confidential nature of the Service Personal Data and comply with the obligations set out in this Clause;

CO-3.4.6 ensure that none of the Supplier Staff publish, disclose or divulge Customer's Personal Data to any third party unless necessary for the provision of the G-Cloud Services under the Call-Off Agreement and/or directed in writing to do so by the Customer;

CO-3.4.7 notify the Customer within five (5) Working Days if it receives:

CO-3.4.7.1 a request from a Data Subject to have access to Service Personal Data relating to that person; or

CO-3.4.7.2 a complaint or request relating to the Customer's obligations under the Data Protection Legislation;

CO-3.4.8 provide the Customer with full cooperation and assistance in relation to any complaint or request made relating to Service Personal Data, including by:

CO-3.4.8.1 providing the Customer with full details of the complaint or request;

CO-3.4.8.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Customer's instructions;

CO-3.4.8.3 providing the Customer with any Service Personal Data it holds in relation to a Data Subject (within the timescales required by the Customer); and

CO-3.4.8.4 providing the Customer with any information requested by the Data Subject.

CO-3.5 The Supplier shall:

CO-3.5.1 permit the Customer or the Customer's Representative (subject to the reasonable and appropriate confidentiality undertakings), to inspect and audit the Supplier's data Processing activities (and/or those of its agents, subsidiaries and Sub-Contractors) or provide to the Customer an independent third party inspection and audit certificate in lieu of the same and shall comply with all reasonable requests or directions by the Customer to enable the Customer to verify and/or procure that the Supplier is in full compliance with its obligations under this Call-Off Agreement; and/or

CO-3.5.2 subject to Clause CO-3.6 agree to an appointment of an independent auditor selected by the Supplier to undertake the activities in Clause CO-3.5.1 provided such selection is acceptable to the Customer or Customer Representative (subject to such independent auditor complying with the reasonable and appropriate confidentiality undertakings).

CO-3.6 The Supplier Shall:

CO-3.6.1 obtain prior written consent from the Customer in order to transfer Customer Personal Data to any other person (including for the avoidance of doubt any Sub-Contractors) for the provision of the G-Cloud Services;

CO-3.6.2 not cause or permit to be Processed, stored, accessed or otherwise transferred outside the EEA any Customer Personal Data supplied to it by the Customer without the prior written consent of the Customer. Where the Customer consents to such Processing, storing, accessing or transfer outside the European Economic Area the Supplier shall:

CO-3.6.2.1 comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is so processed, stored, accessed or transferred;

CO-3.6.2.2 comply with any reasonable instructions notified to it by the Customer and either:

CO-3.6.2.3 incorporate standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) or warrant that that the obligations set out in the Supplier Terms provide Adequate protection for Personal Data.

CO-3.7 The Supplier shall not perform its obligations under this Call-Off Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the Data Protection Legislation.

CO-3.8 The Supplier acknowledges that, in the event that it breaches (or attempts or threatens to breach) its obligations relating to Customer Personal Data that the Customer may be irreparably harmed (including harm to its reputation). In such circumstances, the Customer may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).

CO-4 CONFIDENTIALITY

CO-4.1 Except to the extent set out in this Clause or where disclosure is expressly permitted elsewhere in this Call-Off Agreement, each Party shall:

CO-4.1.1 treat the other Party's Confidential Information as confidential and safeguard it accordingly; and

CO-4.1.2 not disclose any Confidential Information belonging to the other Party to any other person without the prior written consent of the other Party, except to such persons and to such extent as may be necessary for the performance of this Call-Off Agreement.

CO-4.2 The Supplier may only disclose the Customer's Confidential Information to the Supplier Staff who are directly involved in the provision of the G-Cloud Services and who need to know the information, and shall ensure that such Supplier Staff are aware of and shall comply with these obligations as to confidentiality.

CO-4.3 The Supplier shall not, and shall procure that the Supplier Staff do not, use any of the Customer's Confidential Information received otherwise than for the purposes of this Call-Off Agreement.

CO-4.4 The provisions of Clauses CO-4.1 shall not apply to the extent that:

CO-4.4.1 such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under Clause CO-7 (Transparency) and the FOIA, the Ministry of Justice Code or the Environmental Information Regulations pursuant to Clause CO-6 (Freedom of Information);

CO-4.4.2 such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

CO-4.4.3 such information was obtained from a third party without obligation of confidentiality;

CO-4.4.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Call-Off Agreement; or

CO-4.4.5 it is independently developed without access to the other Party's Confidential Information.

CO-4.5 Nothing in this Call-Off Agreement shall prevent the Customer from disclosing the Supplier's Confidential Information (including the Management Information obtained under Clause FW-8 (Provision of Management Information) of the Framework Agreement):

CO-4.5.1 for the purpose of the examination and certification of the Customer's accounts;

CO-4.5.2 for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Customer has used its resources;

CO-4.5.3 to any Crown body or any Other Contracting Body. All Crown bodies or Contracting Bodies receiving such Supplier's Confidential Information shall be entitled to further disclose the Supplier's Confidential Information to other Crown bodies or Other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown body or any Contracting Body; or

CO-4.5.4 to any consultant, contractor or other person engaged by the Customer (on the basis that the information shall be held by such consultant, contractor or other person in confidence and is not to be disclosed to any third party) or any person conducting a Cabinet Office or ERG Gateway review or any additional assurance programme.

CO-4.6 In the event that the Supplier fails to comply with Clauses CO-4.1 to Clause CO-4.4, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by notice in writing.

CO-4.7 In order to ensure that no unauthorised person gains access to any Confidential Information or any data obtained in performance of this Call-Off Agreement, the Supplier undertakes to maintain adequate security arrangements that meet the requirements of Good Industry Practice.

CO-4.8 The Supplier will immediately notify the Customer of any breach of security in relation to Customer Confidential Information obtained in the performance of this Call-Off Agreement and will keep a record of such breaches. The Supplier will use its best endeavours to recover such Customer Confidential Information however it may be recorded. This obligation is in addition to the Supplier's

obligations under Clauses CO-4.1 to Clause CO-4.4. The Supplier will co-operate with the Customer in any investigation that the Customer considers necessary to undertake as a result of any breach of security in relation to Customer Confidential Information.

CO-4.9 Subject always to Clause CO-11.4 the Supplier shall, at all times during and after the Call-Off Agreement Period, indemnify the Customer and keep the Customer fully indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against the Customer arising from any breach of the Supplier's obligations under the DPA or this Clause CO-4 (Confidentiality) except and to the extent that such liabilities have resulted directly from the Customer's instructions.

CO-5 CUSTOMER DATA

CO-5.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Customer Data.

CO-5.2 The Supplier shall not store, copy, disclose, or use the Customer Data except as necessary for the performance by the Supplier of its obligations under this Call-Off Agreement or as otherwise expressly approved by the Customer.

CO-5.3 The Supplier shall ensure that any system on which the Supplier holds any Customer Data, including back-up data, is a secure system that complies with the Supplier security policy.

STATUTORY OBLIGATIONS AND REGULATIONS

CO-6 FREEDOM OF INFORMATION

CO-6.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and co-operate with the Customer to enable the Customer to comply with its Information disclosure obligations.

CO-6.2 The Supplier shall:

CO-6.2.1 transfer to the Customer all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receiving a Request for Information;

CO-6.2.2 provide the Customer with a copy of all Information, relating to a Request for Information, in its possession or control, in the form that the Customer requires within five (5) Working Days (or such other period as the Customer may specify) of the Customer's request; and

CO-6.2.3 provide all necessary assistance as reasonably requested by the Customer to enable the Customer to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

CO-6.3 The Customer shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Call-Off Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information (including Supplier's Confidential Information) is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

CO-6.4 In no event shall the Supplier respond directly to a Request for Information unless authorised in writing to do so by the Customer.

CO-6.5 The Supplier acknowledges that the Customer may, acting in accordance with the Ministry of Justice Code, be obliged under the FOIA, or the Environmental Information Regulations to disclose Information concerning the Supplier or the G-Cloud Services:

CO-6.5.1 in certain circumstances without consulting the Supplier; or

CO-6.5.2 following consultation with the Supplier and having taken its views into account;

provided always that where Clause CO-6.5.1 applies the Customer shall, in accordance with any recommendations of the Ministry of Justice Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

CO-6.5.3 The Supplier acknowledges that the description of information as Commercially Sensitive Information in Framework Schedule 6 (Interpretations and Definitions) is of an indicative nature only and that the Customer may be obliged to disclose it in accordance with this Clause CO-6.

CO-7 TRANSPARENCY

CO-7.1 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Call-Off Agreement is not Confidential Information. The Customer shall be responsible for determining in its absolute discretion whether any of the content of this Call-Off Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

CO-7.2 Notwithstanding any other term of this Call-Off Agreement, the Supplier hereby gives its consent for the Customer to publish this Call-Off Agreement in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted), including from time to time agreed changes to this Call-Off Agreement, to the general public.

CO-7.3 The Customer may consult with the Supplier to inform its decision regarding any redactions but the Customer shall have the final decision in its absolute discretion.

CO-7.4 The Supplier shall assist and cooperate with the Customer to enable the Customer to publish this Call-Off Agreement.

CO-8 OFFICIAL SECRETS ACTS

CO-8.1 The Supplier shall comply with and shall ensure that the Supplier Staff comply with, the provisions of:

CO-8.1.1 the Official Secrets Act 1911 to 1989; and

CO-8.1.2 Section 182 of the Finance Act 1989.

CO-8.2 In the event that the Supplier or the Supplier Staff fails to comply with this Clause, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by giving notice in writing to the Supplier.

CO-9 TERM AND TERMINATION

CO-9.1 This Call-Off Agreement shall take effect on the Effective Date and shall expire on:

CO-9.1.1 the date specified in paragraph 1.2 of the Order Form; or

CO-9.1.2 twenty four (24) Months after the Effective Date, whichever is the earlier, unless terminated earlier pursuant to this Clause CO-9.

CO-9.2 Termination without Cause

CO-9.2.1 The Customer shall have the right to terminate this Call-Off Agreement at any time by giving the length of written notice to the Supplier as set out in paragraph 10.2 of the Order Form.

CO-9.3 Termination on Change of Control

CO-9.3.1 The Supplier shall notify the Customer immediately if the Supplier undergoes a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 (**"Change of Control"**) and provided this does not contravene any Law shall notify the Customer immediately in writing of any circumstances suggesting that a Change of Control is planned or in contemplation. The Customer may terminate the Call-Off Agreement by notice in writing with immediate effect within six (6) Months of:

CO-9.3.1.1 being notified in writing that a Change of Control has occurred or is planned or in contemplation; or

CO-9.3.1.2 where no notification has been made, the date that the Customer becomes aware of the Change of Control,

but shall not be permitted to terminate where a written approval was granted prior to the Change of Control.

CO-9.3.2 For the purposes of Clause CO-9.3.1, any transfer of shares or of any interest in shares by its affiliate company where such transfer forms part of a bona fide reorganisation or restructuring shall be disregarded.

CO-9.4 Termination by Supplier

CO-9.4.1 If the Customer fails to pay the Supplier undisputed sums of money when due, the Supplier shall notify the Customer in writing of such failure to pay and allow the Customer five (5) calendar days to settle undisputed invoice. If the Customer fails to pay such undisputed sums within allotted additional 5 calendar days, the Supplier may terminate this Call-Off Agreement subject to giving the length of notice as specified in paragraph 10.1 of the Order Form.

CO-9.5 Termination on Insolvency

CO-9.5.1 The Customer may terminate this Call-Off Agreement with immediate effect by notice in writing where the Supplier:

CO-9.5.1.1 being an individual, or where the Supplier is a firm, any partner or partners in that firm who together are able to exercise direct or indirect control, as defined by Section 416 of the Income and Corporation Taxes Act 1988, and:

CO-9.5.1.2 shall at any time become bankrupt or shall have a receiving order or administration order made against him or shall make any composition or arrangement with or for the benefit of his creditors, or shall make any conveyance or assignment for the benefit of his creditors, or shall purport so to do, or appears unable to pay or to have no reasonable prospect of being able to pay a debt within the meaning of Section 268 of the Insolvency Act 1986, or any similar event occurs under the law of any other jurisdiction; or

CO-9.5.1.3 a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such attachment or process is not discharged within fourteen (14) calendar days; or

CO-9.5.1.4 he dies or is adjudged incapable of managing his affairs within the meaning of Part VII of the Mental Health Act 1983; or

CO-9.5.1.5 the Supplier suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.

CO-9.5.2 being a company, passes a resolution, or the Court makes an order that the Supplier or its Parent Company be wound up otherwise than for the purpose of a bona fide

reconstruction or amalgamation, or a receiver, manager or administrator on behalf of a creditor is appointed in respect of the business or any part thereof of the Supplier or its Parent Company (or an application for the appointment of an administrator is made or notice to appoint an administrator is given in relation to the Supplier or its Parent Company), or circumstances arise which entitle the Court or a creditor to appoint a receiver, manager or administrator or which entitle the Court otherwise than for the purpose of a bona fide reconstruction or amalgamation to make a winding-up order, or the Supplier or its Parent Company is unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986 (except where the claim is made under Section 123(1)(a) and is for an amount of less than ten thousand pounds (£10,000)) or any similar event occurs under the law of any other jurisdiction.

CO-9.6 Termination on Material Breach

CO-9.6.1 The Customer may terminate this Call-Off Agreement with immediate effect by giving written notice to the Supplier if the Supplier commits a Material Breach of any obligation under this Call-Off Agreement and if:

CO-9.6.1.1 the Supplier has not remedied the Material Breach within thirty (30) Working Days (or such other longer period as may be specified by the Customer) of written notice to the Supplier specifying the Material Breach and requiring its remedy; or

CO-9.6.1.2 the Material Breach is not, in the opinion of the Customer capable of remedy.

CO-9.7 Termination for repeated Default

CO-9.7.1 If there are two or more Defaults (of a similar nature) that will be deemed a breach for Material Breach. Where the Customer considers that the Supplier has committed a repeated Default in relation to this Call-Off Agreement or any part thereof (including any part of the G-Cloud Services) and believes that the Default is remediable, then the Customer shall be entitled to serve a notice on the Supplier:

CO-9.7.1.1 specifying that it is a formal warning notice;

CO-9.7.1.2 giving reasonable details of the breach; and

CO-9.7.1.3 stating that such breach is a breach which, if it recurs or continues, may result in a termination of this Call-Off Agreement or that part of the G-Cloud Services affected by such breach.

CO-9.7.2 If, thirty (30) Working Days after service of a formal warning notice as described in Clause CO-9.7, the Supplier has failed to demonstrate to the satisfaction of the Customer that the breach specified has not continued or recurred and that the Supplier has put in place measures to ensure that such breach does not recur, then the Customer may deem such failure to be a Material Breach not capable of remedy for the purposes of Clause CO-9.6.1.2.

CO-9.8 The termination (howsoever arising) or expiry of this Call-Off Agreement pursuant to this Clause 9 shall be without prejudice to any rights of either the Customer or the Supplier that shall have accrued before the date of such termination or expiry.

CO-9.9 Save as aforesaid, the Supplier shall not be entitled to any payment from the Customer after the termination (howsoever arising) or expiry of this Call-Off Agreement.

CO-10 CONSEQUENCES OF SUSPENSION, TERMINATION AND EXPIRY

CO-10.1 Where a Customer has the right to terminate a Call-Off Agreement, it may elect to suspend this Call-Off Agreement and its performance.

CO-10.2 Notwithstanding the service of a notice to terminate this Call-Off Agreement or any part thereof, the Supplier shall continue to provide the Ordered G-Cloud Services until the date of expiry or termination (howsoever arising) of this Call-Off Agreement (or any part thereof) or such other date as required under this Clause CO-10.

CO-10.3 Within ten (10) Working Days of the earlier of the date of expiry or termination (howsoever arising) of this Call-Off Agreement, the Supplier shall return (or make available) to the Customer:

CO-10.3.1 any data (including (if any) Customer Data), Customer Personal Data and Customer Confidential Information in the Supplier's possession, power or control, either in its then current format or in a format nominated by the Customer (in which event the Customer will reimburse the Supplier's pre-agreed and reasonable data conversion expenses), together with all training manuals, access keys and other related documentation, and any other information and all copies thereof owned by the Customer, save that it may keep one copy of any such data or information for a period of up to twelve (12) Months to comply with its obligations under the Framework Schedule FW-5, or such period as is necessary for such compliance (after which time the data must be deleted); and

CO-10.3.2 any sums prepaid in respect of Ordered G-Cloud Services not provided by the date of expiry or termination (howsoever arising) of this Call-Off Agreement.

CO-10.4 The Customer and the Supplier shall comply with the exit and service transfer arrangements as per the Supplier's terms and conditions identified in Framework Schedule 1 (G-Cloud Services).

CO-10.5 Subject to Clause CO-11 (Liability), where the Customer terminates this Call-Off Agreement under Clause CO-9.2 (Termination without Cause), the Customer shall indemnify the Supplier against any reasonable and proven commitments, liabilities or expenditure which would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Call-Off Agreement, provided that the Supplier takes all reasonable steps to mitigate such loss. Where the Supplier holds insurance, the Supplier shall reduce its unavoidable costs by any insurance sums available. The Supplier shall submit a fully itemised and costed list of such loss, with supporting evidence, of losses reasonably and actually incurred by the Supplier as a result of termination under Clause CO-9.2 (Termination without Cause).

CO-11 LIABILITY

CO-11.1 Nothing in this Clause CO-11 shall affect a Party's general duty to mitigate its loss.

CO-11.2 Nothing in this Call-Off Agreement shall be construed to limit or exclude either Party's liability for:

CO-11.2.1 death or personal injury caused by its negligence or that of its staff;

CO-11.2.2 bribery, Fraud or fraudulent misrepresentation by it or that of its staff;

CO-11.2.3 any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982; or

CO-11.2.4 any other matter which, by Law, may not be excluded or limited.

CO-11.3 Nothing in this Call-Off Agreement shall impose any liability on the Customer in respect of any liability incurred by the Supplier to any other person, but this shall not be taken to exclude or limit any liability of the Customer to the Supplier that may arise by virtue of either a breach of the Call-Off Agreement or by negligence on the part of the Customer, or the Customer's employees, servants or agents.

CO-11.4 Subject always to Clause CO-11.2, the aggregate liability of either Party under or in connection with each Year of this Call-Off Agreement (whether expressed as an indemnity or otherwise):

CO-11.4.1 for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to the Customer Personal Data or Customer Data) of the other Party, shall be subject to the financial limits set out in paragraph 8.1 of the Order Form;

CO-11.4.2 and in respect of all other defaults, claims, losses or damages, whether arising from breach of contract, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall not exceed a sum equivalent to the financial limit set out in paragraph 8.3 of the Order Form .

CO-11.5 Subject always to Clause CO-11.4 the Customer shall have the right to recover as a direct loss:

CO-11.5.1 any additional operational and/or administrative expenses arising from the Supplier's Default;

CO-11.5.2 any wasted expenditure or charges rendered unnecessary and/or incurred by the Customer arising from the Supplier's Default; and

CO-11.5.3 any losses, costs, damages, expenses or other liabilities suffered or incurred by the Customer which arise out of or in connection with the loss of, corruption or damage to or failure to deliver Customer Data by the Supplier.

CO-11.6 The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Call-Off Agreement.

CO-11.7 Subject to Clauses CO-11.2 and Clause CO-11.5, in no event shall either Party be liable to the other for any:

CO-11.7.1 loss of profits;

CO-11.7.2 loss of business;

CO-11.7.3 loss of revenue;

CO-11.7.4 loss of or damage to goodwill;

CO-11.7.5 loss of savings (whether anticipated or otherwise); and/or

CO-11.7.6 any indirect, special or consequential loss or damage.

CO-11.8 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall be subject to the financial limits set out in paragraph 8.2 of the Order Form.

CO-12 INSURANCE

CO-12.1 The Supplier shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under this Call-Off Agreement, including death or personal injury, loss of or damage to property or any other loss (including the insurance policies specified in the relevant paragraph of the Order Form). Such policies shall include cover in respect of any financial loss arising from any advice given or omitted to be given by the Supplier. Such insurance shall be maintained for the Call-Off Agreement Period and for the minimum insurance period as set out in paragraph 9 of the Order Form.

CO-12.2 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under this Call-Off Agreement.

CO-13 PAYMENT, VAT AND CALL-OFF AGREEMENT CHARGES

CO-13.1 In consideration of the Supplier's performance of its obligations under this Call-Off Agreement, the Customer shall pay the Charges in accordance with the Clause CO-13.2 to CO-13.8.

CO-13.2 The Customer shall pay all sums properly due and payable to the Supplier in cleared funds within the time period specified in paragraph 6 of the Order Form.

CO-13.3 The Supplier shall ensure that each invoice contains all appropriate references and a detailed breakdown of the G-Cloud Services supplied and that it is supported by any other documentation reasonably required by the Customer to substantiate the invoice.

CO-13.4 Where the Supplier enters into a Sub-Contract it shall ensure that a provision is included in such Sub-Contract which requires payment to be made of all sums due by the Supplier to the Sub-Contractor within a specified period not exceeding thirty (30) calendar days from the receipt of a validly issued invoice, in accordance with the terms of the Sub-Contract.

CO-13.5 The Supplier shall add VAT to the Charges at the prevailing rate as applicable.

CO-13.6 The Supplier shall fully indemnify the Customer on demand and keep the Customer fully indemnified on a continuing basis against any liability, including without limitation against any interest, penalties or costs, which are suffered or incurred by or levied, demanded or assessed on the Customer at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Call-Off Agreement. Any amounts due under this Clause CO-13 shall be paid by the Supplier to the Customer not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Customer.

CO-13.7 The Supplier shall not suspend the supply of the G-Cloud Services unless the Supplier is entitled to terminate this Call-Off Agreement under Clause CO-9.4 for Customer's failure to pay undisputed sums of money. Interest shall be payable by the Customer on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

CO-13.8 In the event of a disputed invoice, the Customer shall make payment in respect of any undisputed amount in accordance with the provisions of Clause CO-13 of this Call-Off Agreement and return the invoice to the Supplier within ten (10) Working Days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The Supplier shall respond within ten (10) Working Days of receipt of the returned invoice stating whether or not the Supplier accepts the Customer's proposed amendments. If it does then the Supplier shall supply with the response a replacement valid invoice.

CO-13.9 The Supplier shall accept the Government Procurement Card as a means of payment for the G-Cloud Services where such card is agreed with the Customer to be a suitable means of payment. The Supplier shall be solely liable to pay any merchant fee levied for using the Government Procurement Card and shall not be entitled to recover this charge from the Customer.

CO-14 GUARANTEE

CO-14.1 Where the Customer has specified in the Order Form that this Call-Off Agreement shall be conditional upon receipt of a Guarantee from the guarantor, the Supplier shall deliver to the Customer an executed Guarantee from the guarantor, on or prior to the Commencement Date; and deliver to the Customer a certified copy of the passed resolution and/or board minutes of the guarantor approving the execution of the Guarantee.

CO-15 FORCE MAJEURE

CO-15.1 Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Agreement to the extent that such delay or failure is a result of Force Majeure.

CO-15.2 Notwithstanding Clause CO-15.1, each Party shall use all reasonable endeavours to continue to perform its obligations under the Call-Off Agreement for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under this Call-Off Agreement for a period in excess of one hundred and twenty (120) calendar days, either Party may terminate this Call-Off Agreement with immediate effect by notice in writing to the other Party.

CO-16 TRANSFER AND SUB-CONTRACTING

CO-16.1 The Supplier shall not assign, novate, sub-contract or in any other way dispose of this Call-Off Agreement or any part of it without the Customer's prior written approval which shall not be unreasonably withheld or delayed. Sub-Contracting any part of this Call-Off Agreement shall not relieve the Supplier of any obligation or duty attributable to the Supplier under this Call-Off Agreement.

CO-16.2 The Supplier shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own.

CO-16.3 The Customer may assign, novate or otherwise dispose of its rights and obligations under the Call-Off Agreement or any part thereof to:

CO-16.3.1 any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Customer; or

CO-16.3.2 any private sector body which substantially performs the functions of the Customer

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

CO-17 THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

CO-17.1 A person who is not party to this Call-Off Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Call-Off Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

CO-18 LAW & JURISDICTION

CO-18.1 This Call-Off Agreement and/or any non-contractual obligations or matters arising out of or in connection with it, shall be governed by and construed in accordance with the Laws of England and Wales and without prejudice to the dispute resolution procedures set out in Clause FW-14 or CO-22 (Dispute Resolution) each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

CO-19 ADDITIONAL G-CLOUD SERVICES

CO-19.1 The Customer may require the Supplier to provide the Additional G-Cloud Services. The Supplier acknowledges that the Customer is not obliged to take any Additional G-Cloud Services from the Supplier and that there is nothing preventing the Customer from receiving services that are the same as or similar to the Additional G-Cloud Services from any third party.

CO-19.2 The Supplier shall provide Additional G-Cloud Services in accordance with any relevant Implementation Plan(s) and the Supplier shall monitor the performance of such Additional G-Cloud Services against the Implementation Plan(s).

CO-20 [COLLABORATION AGREEMENT

CO-20.1 Where the Customer has specified in paragraph 13 of the Order Form that the Customer requires the Supplier to enter into a Collaboration Agreement, a Collaboration Agreement should be executed between the Parties, on or prior to the Commencement Date.

CO-20.2 In addition to its obligations under any Collaboration Agreement, the Supplier shall:

CO-20.2.1 work pro-actively with each of the Customer's contractors in a spirit of trust and mutual confidence;

CO-20.2.2 in addition to its obligations under the Collaboration Agreement the Supplier shall cooperate with the Customer's contractors of other services to enable the efficient operation of the ICT services; and

CO-20.2.3 assist in sharing information with the Customer's contractors for the purposes of facilitating adequate provision of the G-Cloud Services and/or Additional G-Cloud Services.]

CO-21 VARIATION PROCEDURE

CO-21.1 The Customer may request in writing a variation to this Call-Off Agreement provided that such variation does not amount to a material change of the Framework Agreement and/or this Call-Off Agreement and is within the meaning of the Regulations and the Law. Such a change once implemented is hereinafter called a **"Variation"**.

CO-21.2 The Supplier shall notify the Customer immediately in writing of any changes proposed or in contemplation in relation to G-Cloud Services or their delivery by submitting Variation request. For the avoidance of doubt such changes would include any changes within the Supplier's supply chain.

CO-21.3 In the event that:

(a) Either Party is unable to agree (agreement shall not be unreasonably withheld or delayed) to or provide the Variation;

(b) the Customer may:

(i) agree to continue to perform its obligations under this Call-Off Agreement without the Variation; or

(ii) terminate this Call-Off Agreement by giving thirty (30) written days notice to the Supplier.

CO-22 DISPUTE RESOLUTION

CO-22.1 The Customer and the Supplier shall attempt in good faith to negotiate a settlement of any dispute between them arising out of or in connection with this Call-Off Agreement within twenty (20) Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the Customer Representative and the Supplier Representative.

CO-22.2 If the dispute cannot be resolved by the Parties pursuant to this Clause, the Parties shall refer it to mediation unless the Customer considers that the dispute is not suitable for resolution by mediation.

CO-22.3 If the dispute cannot be resolved by mediation the Parties may refer it to arbitration.

CO-22.4 The obligations of the Parties under this Call-Off Agreement shall not be suspended, cease or be delayed by the reference of a dispute to mediation or arbitration pursuant to this Clause and the Supplier and Supplier's Staff shall continue to comply fully with the requirements of this Call-Off Agreement at all times.

Schedule 3: Call-Off Ordering Procedure

S3-1 BACKGROUND

S3-1.1 All Call-Off Agreements from this Framework Agreement will be conducted using the Digital Marketplace.

S3-1.2 All Call-Off Agreements from this Framework Agreement will apply the award criteria stipulated in this Framework Schedule 3.

S3-2 CATALOGUE – LOTS 1-4

S3-2.1 The Catalogue provides the list of products which may be required by Other Contracting Bodies during the Term and any Call-Off Agreements. The products are listed in Schedule 1 (G-Cloud Services) according to the respective G-Cloud Services on offer in Lots 1-4.

S3-2.2 The Authority shall create a Catalogue for the G-Cloud Services in each Lot where a Framework Supplier has been awarded a place on the Framework Agreement. The Catalogues shall include each of the individual G-Cloud Services as specified in the Schedule 1 (G-Cloud Services).

S3-2.3 The structure of the Catalogue shall comprise of a number of menu and content pages which set out all relevant details of the G-Cloud Services offered within each Lot.

S3-3 PROCESS – DIRECT AWARD LOWEST PRICE

S3-3.1 If the Authority or any Contracting Body decides to source the G-Cloud Services through this Framework Agreement then it will award its Call-Off Agreement in accordance with the procedure in this Framework Schedule 3 (Ordering Procedure) and the requirements of the Regulations and the Guidance.

S3-3.2 The Customer would use a credit reference agency (currently Experian) as the first step in assessing Supplier's economic and financial standing and the report provided by a credit agency will be used to determine the level of financial risk the Supplier would represent. If the Customer determines that the Supplier's financial risk is determined as being above (i.e. worse than) average the Supplier will not be successful in their award.

S3-3.3 Subject to paragraph S3-3.1, any Contracting Body ordering the G-Cloud Services under this Framework Agreement shall:

S3-3.3.1 Apply Long-Listing -

in the first instance and would have to derive a long-list of service offerings which meet their essential minimum requirements.

S3-3.3.2 Apply Short-Listing -

Contracting Bodies will then proceed to reduce this list of service offerings down to a short-list. They will short-list those offerings which provide a suitable service within the available budget of the Contracting Body.

S3-3.4 Contracting Bodies may at this point directly award to the Framework Supplier with the lowest price.

S3-4 PROCESS – DIRECT AWARD: MOST ECONOMICALLY ADVANTAGEOUS TENDER (MEAT)

S3-4.1 In the event that Contracting Bodies are unable to identify which service best meets their needs purely on the basis of an evaluation of price then all short-listed offerings will be compared to the Customer's service requirements.

S3-4.2 The Customer would use a credit reference agency (currently Experian) as the first step in assessing Supplier's economic and financial standing and the report provided by a credit agency will be used to determine the level of financial risk the Supplier would represent. If the Customer determines that the

Supplier's financial risk is determined as being above (i.e. worse than) average the Supplier will not be successful in their award.

S3-4.3 The evaluation model must apply the following evaluation criteria albeit Contracting Bodies may apply their own weighting to each of the criteria:

Criteria Number	Direct Award Criteria
1	Whole life cost: cost effectiveness; price and running costs;
2	Technical merit & functional fit: coverage, network capacity and performance as specified in relevant service levels;
3	After sales service management: help desk, account management function and assurance of supply of a range of services; and
4	Non-functional characteristics.

S3-4.4 Contracting Bodies are permitted to conduct such tests and demonstrations or set service definitions or standards as are necessary to enable them to establish which of the short-listed offerings provides the most economically advantageous solution to their needs. In the first instance, Service Definitions will provide appropriate information.

S3-4.5 All short-listed offerings must be evaluated against the same evaluation model.

S3-4.7 Where a Call-Off Agreement is awarded following the direct award process outlined in this paragraph S3-4 in this Framework Schedule 3 the Contracting Body shall notify all short-listed Suppliers that did not succeed that they have been considered for award, and inform those how their offering(s) performed on the evaluation.

Schedule 4: Management Information Requirements

S4-1 AUTHORITY REPORTING REQUIREMENTS (FRAMEWORK AGREEMENT)

S4-1.1 The Authority shall provide the Supplier with a template report by email prior to or shortly after by the first Working Day of each Month (**"Monthly email"**). It is the responsibility of the Authority to provide the Supplier with an up to date template report. Templates from previous Months should not be used as the date will be incorrect and the Authority's system will not accept it. An example of the template report current at the date of this Framework Agreement is available from the e-Tendering Portal.

S4-1.2 The Authority shall provide guidance notes for completing the template report and shall update them from time to time. The template report should be completed by the Supplier in accordance with the guidance notes. Some fields in the template report are mandatory and these fields will be highlighted in the guidance notes. Returns will not be accepted unless all mandatory fields have been completed by the Supplier.

S4-1.3 The Supplier undertakes to provide timely, full, accurate and complete Management Information (**"MI"**) reports to the Authority which incorporates the data, in the correct format, required by the MI reporting template. The initial reporting template is set out in the Annex to this Framework Schedule 4.

S4-1.4 The Supplier may not make any amendment to the current MI reporting Template without the prior Approval.

S4-1.5 The Authority shall have the right from time to time (on reasonable written notice) to amend the nature of the Management Information which the Supplier is required to supply to the Authority.

S4-1.6 The template report should be used to report Orders received, invoices raised during the Month that is being reporting on, regardless of when the work was actually done (e.g. if the invoice was raised in October but the work that was invoiced was done in September the Supplier should report the invoice in October's return not September's). Business should be reported once only as an Order and once again as an invoice, where the Order and the invoice take place in different Months. The Supplier should also inform the Authority of any corrections to previous Months' Management Information. No amendment should be made to the current template report without the prior notification and the Approval.

S4-1.7 Any errors or omissions may result in the return being rejected and an administration charge being added to the Management Charge invoice.

S4-1.8 The Supplier must return the template by 7th day of each Month including where there has been no activity in the relevant Month ("nil returns"). Where the 7th day falls on a weekend or public holiday then the nearest Working Day before the 7th day.

S4-1.9 The completed template should be returned to the sender of the Monthly email or as otherwise communicated to the Supplier from time to time. In the subject line of the return email the Supplier must insert this Framework number, the Supplier's name and the Month that the return relates to.

S4-1.10 The deadline for the return of the template is the Reporting Date provided for in this Framework Agreement. If a return has not been received by the deadline the Supplier will be contacted by a member of the Authority's data team and an administration charge may be added to the relevant invoice.

S4-1.11 MI Failure is when an MI Report:

S4-1.11.1 contains any material errors or material omissions or a missing mandatory field; or

S4-1.11.2 is submitted using an incorrect MI reporting template; or

S4-1.11.3 is not submitted by the Reporting Date (including where a Nil Return should have been filed); or

S4-1.11.4 then the Authority may deem the failure to submit an MI Report correctly as an **"MI Failure"**.

S4-1.12 Following an MI Failure the Authority may issue reminders to the Supplier or require the Supplier to rectify defects in the MI Report provided to the Authority. The Supplier shall rectify any deficient or incomplete MI Report as soon as possible and not more than five (5) Working Days following receipt of any such reminder.

S4-2 ADMIN FEES

S4-2.1 If, in any rolling three (3) Month period, two (2) or more MI Failures occur, the Supplier acknowledges and agrees that the Authority shall have the right to invoice the Supplier Admin Fees and (subject to paragraph S4-1.11) in respect of any MI Failures as they arise in subsequent Months.

S4-2.2 If, following activation of the Authority's right to charge Admin Fee(s) in respect of MI Failures pursuant to paragraph S4-2.1, the Supplier submits the Monthly MI Report for two (2) consecutive Months and no MI Failure occurs then the right to charge the Admin Fee(s) shall lapse. For the avoidance of doubt the Authority shall not be prevented from exercising such right again during the Term if the conditions in paragraph S4-2.1 are met.

S4-2.3 The Supplier acknowledges and agrees that the Admin Fees are a fair reflection of the additional costs incurred by the Authority as a result of the Supplier failing to supply Management Information as required by this Framework Agreement.

S4-2.4 Authority shall notify the Supplier if any Admin Fees arise pursuant to paragraph S4-2.1 above and shall be entitled to invoice the Supplier for such Admin Fees which shall be payable in accordance with FW-9 as a supplement to the Management Charge. Any exercise by the Authority of its rights under this paragraph shall be without prejudice to any other rights that may arise pursuant to the terms of the Framework Agreement.

ANNEX A: MI REPORTING TEMPLATE

Schedule 5: Records and Audit Access

S5-1.1 The Supplier (which for the purposes of this paragraph includes all Sub-Contractors) shall keep and maintain until 12 Months after the date of termination or expiry of this Framework Agreement or of the last Call-Off Agreement (whichever is the later) (or such other period as may be agreed between the Parties), full and accurate records and accounts of the operation of this Framework Agreement including the G-Cloud Services provided under it, the Call-Off Agreements entered into with Contracting Bodies and the amounts paid by each Contracting Body.

S5-1.2 The Supplier shall provide the Authority with a completed Self Audit Certificate at the termination (or expiry) of this Framework Agreement for whatever reason. The Self Audit Certificate shall be completed by responsible senior member of the Supplier's management team or by the Supplier's external auditor or company managing director and shall be provided to the Authority no later than three (3) Months after termination or expiry of this Framework Agreement.

S5-1.3 The Supplier shall afford the Authority, the Authority's representatives, the National Audit Office and/or auditor appointed by the Audit Commission (**"Auditors"**) access to the records and accounts referred to, and for the purposes specified, in paragraph S5-1.1 at the Supplier's premises and/or provide copies of the records and accounts, as may be required and agreed with the Authority (or relevant Other Contracting Body) from time to time, in order that the Authority (or relevant Contracting Body) may carry out an inspection of the records and accounts referred to in paragraph S5-1.1 for the following purposes:

S5-1.3.1 verify the accuracy of Charges (and proposed or actual variations to them in accordance with this Framework Agreement); and

S5-1.3.2 review any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework and Call-Off Agreement only.

S5-1.4 The Supplier shall provide such records and accounts (together with copies of the Supplier's published accounts) on request during the Term and during the Call-Off Agreement Period and for a period of twelve (12) Months after termination or expiry of the Term or the last Call Off Agreement (whichever is the later) to the Authority (or relevant Contracting Body or Auditors) and its internal and external auditors.

S5-1.5 The Authority shall use reasonable endeavours to ensure that the conduct of each Audit does not unreasonably disrupt the Supplier or delay the provision of the G-Cloud Services pursuant to the Call-Off Agreements, save insofar as the Supplier accepts and acknowledges that control over the conduct of Audits carried out by the Auditors is outside of the control of the Authority.

S5-1.6 Subject to the Authority's obligations of confidentiality, the Supplier shall on demand provide the Auditors with all reasonable co-operation and assistance in relation to each Audit, including by providing:

S5-1.6.1 all information requested by the Auditor within the scope of the Audit; and

S5-1.6.2 access to the Supplier Staff.

S5-1.7 If an Audit reveals:

S5-1.7.1 an underpayment by the Supplier to the Authority in excess of five (5%) per cent of the total Management Charge due in any monthly reporting and accounting period; and/or

S5-1.7.2 a Material Breach;

then the Supplier shall reimburse the Authority its reasonable costs incurred in relation to the Audit and the Authority shall be entitled to exercise its rights to terminate this Framework Agreement pursuant to Clause FW-12 (Termination).

S5-1.8 Each Party shall bear its own costs and expenses incurred in respect of compliance with its obligations under this Schedule, save as specified in paragraph S5-1.7 of this Schedule 5 of the Framework Agreement.

S5-1.9 Subject to paragraph S5-1.3 of this Schedule, the Supplier may agree to an appointment of an independent auditor selected by the Supplier to undertake the activities in paragraph S5-1.3 of this Schedule 5 provided such selection is Approved by the Authority (and such Approval shall not be unreasonably withheld or delayed).

ANNEX A: SELF AUDIT CERTIFICATE

[To be signed by Head of Internal Audit, Finance Director or company's external auditor]

[Note: To be signed by company's auditor]

Dear Sirs,

In accordance with the Framework Agreement entered into on 26 January 2016 between [insert Supplier name] and the Crown Commercial Service, we confirm the following:

(1) In our opinion [Supplier name] has in place suitable systems for identifying and recording the transactions taking place under the provisions of the above Framework Agreement.

(2) We have tested the systems for identifying and reporting on framework activity and found them to be operating satisfactorily.

(3) We have tested a sample of [ ] [insert number of sample transactions tested] orders and invoices during our audit for the financial year ended [insert financial year] and confirm that they are correct and in accordance with the terms and conditions of the above Framework Agreement.

Signature: .....

Name: Luke Harrop

Position: Director

Date: 4.5.2016

Schedule 6: Interpretations and Definitions

S6-1 INTERPRETATION

S6-1.1 In this Framework Agreement the following expressions have the following meaning:

Adequate	means that the relevant contractual clauses provide sufficient safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26 (2) Directive 95/46/EC and the DPA;
Admin Fees	means those fees defined in paragraph S4-2 of Schedule 4 (Management Information Requirements) of this Framework Agreement;
Approval	means the prior written consent of the Authority and **"Approve"** and **"Approved"** shall be construed accordingly;
Assurance	means the verification process explained in the ITT;
Audit	means an audit carried out pursuant to Schedule 5 (Records and Audit Access) of this Framework Agreement;
Authority Representative	means the representative appointed by the Authority from time to time in relation to this Framework Agreement;
Authority's Confidential Information	means all Authority's Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Authority, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked "confidential");
Authority Personal Data	means the personal data supplied by the Authority to the Supplier and for the purposes of or in connection with this Framework Agreement **"Personal Data"** shall have the same meaning as set out in the Data Protection Act 1998;
Call-Off Agreement	means a legally binding agreement (entered into pursuant to the provisions of this Framework Agreement) for the provision of G-Cloud Services made between a Contracting Body and the Supplier comprising of an Order Form the Call-Off Terms and the Collaboration Agreement;
Call-Off Agreement Period	means the period of the Call-Off Agreement as specified in paragraph 1.1 and 1.2 of the Order Form;
Call-Off Terms	means the terms and conditions (including the Supplier Terms) as set out in Framework Schedule 2 (Call-Off Terms);
Catalogue	means the Digital Marketplace or such or any subsequent pan-government catalogue or such other medium as the Authority may determine;
Charges	means the prices (exclusive of any applicable VAT), payable to the Supplier by the Customer under the Call-Off Agreement, as set out in paragraph 6.1 of the Order Form, in consideration of the full and proper performance by the Supplier of its obligations under the Call-Off Agreement;

Collaboration Agreement	means an agreement between the Customer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Customer's Services and to ensure that the Customer receives an efficient end-to-end G-Cloud Services; such agreement to be in the form set out in Framework Schedule 7 (Collaboration Agreement);
Collaboration Supplier	means a Framework Supplier or the Customer contractor, that has entered into a Collaboration Agreement as set out in Framework Schedule 7 (Collaboration Agreement);
Commencement Date	means a) For the purposes of the Framework Agreement, commencement date shall be 02/02/2015; b) For the purposes of the Call-Off Agreement, commencement date shall be as set out in paragraph 1.1 of the Order Form;
Commercially Sensitive Information	means information provided by the Supplier to the Authority or to the Customer which is a trade secret but this definition does not include the material proposed to be published by the Authority under Clause FW-27 (Transparency)of this Framework Agreement;
Confidential Information	means the Authority's Confidential Information and/or the Supplier's Confidential Information;
Contracting Bodies	means the Authority and any other person as listed in the OJEU Notice or Regulation 3 of the Public Contracts Regulations 2006, as amended from time to time;
Contracting Body Satisfaction Survey	shall have the meaning set out in Clause FW-10 (Contracting Body Satisfaction Monitoring);
Crown	means the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
Customer	means the customer as identified in the Order Form;
Customer's Confidential Information	means all Customer Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Customer, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked "confidential");
Customer Data	means data that is owned or managed by the Customer;
Customer Personal Data	means the Order Personal Data and / or Service Personal Data;
Customer Representative	means the representative appointed by the Customer from time to time in relation to this Call-Off Agreement;
Data Controller	shall have the same meaning as set out in the Data Protection Act 1998, as amended from time to time;

Data Processor	shall have the same meaning as set out in the Data Protection Act 1998, as amended from time to time;
Data Protection Legislation or DPA	means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable legally binding guidance and codes of practice issued by the Information Commissioner;
Data Subject	shall have the same meaning as set out in the Data Protection Act 1998, as amended from time to time;
Default	means any breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or negligent statement of the Supplier in connection with or in relation to this Framework Agreement or the Call-off Agreement and in respect of which the Supplier is liable to the Authority and in relation to the Call-Off Agreement, the Supplier is liable to the Customer;
Direct Award Criteria	means the award criteria to be applied for the award of Call-Off Agreements for G-Cloud Services set out in Framework Schedule 3 (Call-Off Ordering Procedure);
Direct Ordering Procedure	means the ordering procedure set out in Framework Schedule 3 (Call-Off Ordering Procedure);
Effective Date	means the date on which the Call-Off Agreement is signed and as set out in paragraph 1.1 of the Order Form;
Electronic Marketplace	means a web based application which facilitates electronic trade between one or more buying organisations and many suppliers;
Environmental Information Regulations	mean the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such regulations;
ERG	means the Efficiency and Reform Group of the Cabinet Office;
FOIA	means the Freedom of Information Act 2000 and any subordinate legislation made under such Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
Force Majeure	means any event, occurrence or cause affecting the performance by either the Customer or the Supplier of its obligations arising from: a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the affected party; b) riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of government, local government or Regulatory Bodies; d) fire, flood, any disaster and any failure or shortage of power or fuel; e) an industrial dispute affecting a third party for which a substitute third

	party is not reasonably available; provided always that: i. any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Sub-Contractor's supply chain; and ii. any event or occurrence which is attributable to the wilful act, neglect or failure to take reasonable precautions against the event or occurrence by the Party concerned; shall not constitute a Force Majeure;
Framework	means the framework arrangements established by the Authority for the provision of G-Cloud Services to Contracting Bodies by Framework Suppliers;
Framework Agreement	means the Clauses of this Framework Agreement together with the Framework Schedules and annexes to it;
Framework Suppliers	means the suppliers (including the Supplier) appointed under this Framework Agreement;
Fraud	means any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Framework Agreement or defrauding or attempting to defraud or conspiring to defraud the Crown;
G-Cloud Services	means the cloud services described in Framework Schedule 1 (G-Cloud Services) as defined by the Service Definition, the Supplier Terms and any related Tender documentation, which the Supplier shall make available to the Authority and Other Contracting Bodies and those services which are deliverable by the Supplier under the Collaboration Agreement;
G-Cloud Additional Services	means services ancillary to the G-Cloud Services which are within the scope of the Framework Agreement Schedule 1 (G-Cloud Services) which the Customer may request from time to time;
Good Industry Practice	means standards, practices, methods and procedures conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonable and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances;
Guarantee	means the deed of guarantee described in the Order Form (Parent Company Guarantee);
Guidance	means any current UK Government Guidance on the Public Contracts Regulations. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance shall take precedence;
Holding Company	shall have the meaning given to it in section 1159 and Schedule 6 of the Companies Act 2006;
Implementation Plan	means the plan set out in paragraph 12.1 of the Order Form;

Information	has the meaning given under section 84 of the Freedom of Information Act 2000, as amended from time to time;
Intellectual Property Rights or IPR	means: a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and all other rights having equivalent or similar effect in any country or jurisdiction;
Invitation to Tender or ITT	means the invitation to tender for this Framework issued on 6th November 2014;
Know-How	means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or the Authority's possession before the Commencement Date;
Law	means any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body;
Lot	means any of the 4 lots specified in the ITT and "Lots" shall be construed accordingly;
Management Charge	means the sum paid by the Supplier to the Authority being an amount of 0.5% of all Charges for the G-Cloud Services invoiced to Other Contracting Bodies (net of VAT) in each Month throughout the Term and thereafter until the expiry or earlier termination of any Call-Off Agreement;
Management Information	means the management information specified in Framework Schedule 4 (Management Information Requirements);
Material Breach	means: a) a material breach of the Framework Agreement Clause FW-19 and/or breach by the Supplier of the following Clauses in the Framework Agreement: Clause FW-7 (Warranties and Representations), Clause FW-8 (Provision of Management Information), Clause FW-9 (Management Charge), Clause FW-22 (Prevention of Bribery & Corruption), Clause FW-23 (Safeguarding against Fraud), Clause FW-24 (Data Protection & Disclosure), Clause FW-28 (Equality & Diversity), Clause FW-29 (Official Secrets Acts), Schedule 5 (Records and Audits Access); and/or b) a material breach of the Call-Off Agreement and/or breach by the Supplier of any of the following Clauses in the Call-Off Agreement: Clause CO-3 (Protection of Information), C0-4 (Confidentiality), Clause CO-5 (Customer Data), Clause CO-8 (Official Secrets Acts

	1911 to 1989);
Ministry of Justice Code	means the Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000;
Month	means a calendar month and "**Monthly**" shall be interpreted accordingly;
OJEU Notice	means a contract notice in the Official Journal of the European Union, seeking expressions of interest from potential providers of G-Cloud Services;
Order	means an order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Procedures;
Order Form	means the form set out in part 1 of Framework Schedule 2 (Call-Off Terms) to be used by a Contracting Body to order G-Cloud Services;
Ordered G-Cloud Services	means G-Cloud Services which are the subject of an Order by a Contracting Body;
Order Personal Data	means the personal data supplied by the Customer to the Supplier in the course of Ordering the G-Cloud Services for purposes of or in connection with this Call-Off Agreement. "**Personal Data**" shall have the same meaning as set out in the Data Protection Act 1998;
Ordering Procedures	means the ordering and award procedures specified in Framework Schedule 3 (Call-Off Ordering Procedure);
Other Contracting Bodies	means all Contracting Bodies except the Authority;
Parent Company	means any company which is the ultimate Holding Company of the Supplier;
Party	means: a) for the purposes of the Framework Agreement, the Authority or the Supplier; b) for the purposes of the Call-Off Agreement, the Supplier or the Customer; and "**Parties**" shall be interpreted accordingly;
Personal Data	shall have the same meaning as set out in the Data Protection Act 1998;
Processing	has the meaning given to it under the Data Protection Act 1998 as amended from time to time but, for the purposes of this Framework Agreement and Call-Off Agreement, it shall include both manual and automatic processing. "**Process**" and "**Processed**" shall be interpreted accordingly;
Regulations	means the Public Contracts Regulations 2006, as amended from time to time;
Regulatory Bodies	means those government departments and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Framework Agreement or any other affairs of the Authority or Other Contracting Body or the Supplier or its Parent Company;

Relevant Person	means any employee, agent, servant, or representative of the Authority, any other public body or person employed by or on behalf of the Authority, or any other public body;
Reporting Date	means the 7th day of each Month following the Month to which the relevant Management Information relates, or such other date as may be agreed between the Parties;
Request(s) for Information	means a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
Self Audit Certificate	means the certificate in the form as set out in Annex to the Framework Schedule 5 (Self Audit Certificate) to be provided to the Authority in accordance with paragraph S5-1.2 of Schedule 5 (Records and Audit Access);
Service Definition(s)	means the definition of the Supplier's G-Cloud Services provided as part of their Tender that includes, but is not limited to, those items listed in Schedule 1 (G-Cloud Services) of this Framework Agreement;
Service Descriptions	means the description of the Supplier service offering as published on the Catalogue;
Service Personal Data	means the personal data supplied by the Customer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Agreement. **"Personal Data"** shall have the same meaning as set out in the Data Protection Act 1998;
Sub-Contract	means any contract or agreement or proposed agreement between the Supplier and the Sub-Contractor in which Sub-Contractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof;
Sub-Contractor	means any third party engaged by the Supplier from time to time under a Sub-Contract (permitted pursuant to the Framework Agreement and the Call-Off Agreement) and its servants or agents in connection with the provision of the G-Cloud Services from time to time;
Subsidiary	has the meaning given to it in section 1159 of the Companies Act 2006;
Supplier's Confidential Information	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential or which ought reasonably to be considered to be confidential, including the Commercially Sensitive Information (whether or not it is marked as "confidential");
Supplier Representative	means the representative appointed by the Supplier from time to time in relation to this Framework Agreement;
Supplier Terms	means the terms and conditions pertaining to the G-Cloud Services and as set out in Schedule 1 (G-Cloud Services) set in the form supplied as part of the Supplier's Tender;

Supplier Staff	means all persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Sub-Contractors used in the performance of its obligations under this Framework Agreement or any Call-Off Agreements;
Tender	means the response submitted by the Supplier to the Invitation to Tender;
Term	means the term of this Framework Agreement as specified in FW-3 (Term of Framework Agreement);
Variation	has the meaning given to it in Clause CO-21 (Variation Procedure);
Working Days	means any day other than a Saturday, Sunday or public holiday in England and Wales; and
Year	means a contract year.

S6-1.2 The interpretation and construction of this Framework Agreement shall all be subject to the following provisions:

S6-1.2.1 words importing the singular meaning include where the context so admits the plural meaning and vice versa;

S6-1.2.2 words importing the masculine include the feminine and the neuter and vice versa;

S6-1.2.3 the words "include", "includes" "including" "for example" and "in particular" and words of similar effect shall not limit the general effect of the words which precede them;

S6-1.2.4 references to any person shall include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and however constituted and their successors and permitted assigns or transferees;

S6-1.2.5 references to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent enactment, modification, order, regulation or instrument as subsequently amended or re-enacted;

S6-1.2.6 headings are included in this Framework Agreement for ease of reference only and shall not affect the interpretation or construction of this Framework Agreement;

S6-1.2.7 references in this Framework Agreement to any Clause or Framework Schedule without further designation shall be construed as a reference to the Clause or sub-Clause or Schedule to this Framework Agreement so numbered;

S6-1.2.8 references in this Framework Agreement to any paragraph or sub-paragraph without further designation shall be construed as a reference to the paragraph or sub-paragraph of the relevant Framework Schedule to this Framework Agreement so numbered;

S6-1.2.9 reference to a Clause is a reference to the whole of that Clause unless stated otherwise;

S6-1.2.10 where definitions or interpretations are expressly set out in Collaboration Agreement Schedule 7 (Collaboration Agreement), then the definitions and interpretations specified therein shall apply only in the context of the Collaboration Agreement; and

S6-1.2.11 without prejudice to the overriding provisions as detailed in Clause CO-1 of the Framework Schedule 2 (Call-Off Terms) in the event and to the extent only of any conflict between the Clauses and the remainder of the Framework Schedules, the Clauses shall prevail over the remainder.

Schedule 7: Collaboration Agreement

Attached separately

Schedule 8: Implementation Plan

Not Required

Schedule 9: Alternative Clauses

S9-1 INTRODUCTION

S9-1.1 This Schedule specifies the alternative Clauses applying to Scottish Contracting Bodies that may be requested in the Order Form and, if requested in the Order Form, shall apply to this Call-Off Agreement.

S9-2 CLAUSES SELECTED

S9-2.1 The Customer may, in the Order Form, request the following alternative Clauses:

S9-2.1.1 Scots Law (see paragraph S10-2.1.2 of this Schedule);

S9-2.1.2 SCOTS LAW

Law and Jurisdiction (Clause CO-18.1)

References to England and Wales in the original Clause CO-18.1 (Law and Jurisdiction) of this Call-Off Agreement shall be replaced with Scotland.

Reference to England and Wales in Working Days definition within Schedule 6 shall be replaced with Scotland.

References to the Contracts (Rights of Third Parties) Act 1999 shall be removed in Clause CO-17.1.

Reference to the Freedom of Information Act 2000 within definition for FOIA in Schedule 6 – Definitions to be replaced with Freedom of Information (Scotland) Act 2002.

Reference to the Supply of Goods and Services Act 1982 shall be removed in Clause CO-11.2.3.

References to "tort" shall be replaced with "delict" throughout.

S9-2.2 The Customer may, in the Order Form, request the following alternative Clauses:

S9-2.2.1 Northern Ireland Law (see paragraph S10-2.4, 2.5, 2.6 and 2.7 of this Schedule);

S9-2.3 Discrimination.

S9-2.3.1 The Supplier shall comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular, the Employment (Northern Ireland) Order 2002, the Fair Employment and Treatment (Northern Ireland)) Order 1998, the Sex Discrimination (Northern Ireland) Order 1976 and 1988, the Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003, the Equal Pay Act (Northern Ireland) 1970, the Disability Discrimination Act 1995, the Race Relations (Northern Ireland) Order 1997, the Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996 Employment Equality (Age) Regulations (Northern Ireland) 2006; Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000; Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002, The Disability Discrimination (Northern Ireland) Order 2006, The Employment Relations (Northern Ireland) Order 2004, The Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006, The Employment Relations (Northern Ireland) Order 2004 and The Work and Families (Northern Ireland) Order 2006; and shall use his best endeavours to ensure that in his employment policies and

practices and in the delivery of the services required of the Supplier under this Call-Off Agreement he has due regard to the need to promote equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions;

b. men and women or married and unmarried persons;

c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)

d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997);

e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995);

f. persons of different ages; and

g. persons of differing sexual orientation

S9-2.3.2 The Supplier shall take all reasonable steps to secure the observance of Clause S10-2.3.1 by all Supplier Staff.

S9-2.4 Equality Policies and Practices

S9-2.4.1 The Supplier shall introduce and shall procure that any Sub-Contractor shall also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier shall review such policies on a regular basis (and shall procure that its Sub-Contractors do likewise) and the Customer shall be entitled to receive upon request by it a copy of any such policy.

S9-2.4.2 The Supplier shall take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in Clause [S10-2.3] above). These steps shall include:

(a) the issue of written instructions to staff and other relevant persons;

(b) the appointment or designation of a senior manager with responsibility for equal opportunities;

(c) training of all staff and other relevant persons in equal opportunities and harassment matters; and

(d)the inclusion of the topic of equality as an agenda item at team, management and staff meetings,

and the Supplier shall procure that its Sub-Contractors do likewise (in relation to their equal opportunities policies).

S9-2.4.3 In the event of:

(a) the Equality Commission notifying the Supplier of an alleged breach by it or any Sub-Contractor (or any of their shareholders and/or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998; and/or

(b) any finding of unlawful discrimination (or any offence under the Legislation mentioned in Clause S10-2.3 above) being made against the Supplier or its Sub-

Contractors during the Call-Off Agreement Period by any Industrial or Fair Employment Tribunal or Court,

the Supplier shall inform the Customer as soon as reasonably practicable and shall take such steps (including the dismissal or replacement of any relevant staff or Sub-Contractor(s)) as the Customer directs and shall seek the advice of the Equality Commission in order to prevent any such offence or repetition of the unlawful discrimination as the case may be.

S9-2.4.4 The Supplier shall monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and shall provide an annual report on the composition of such workforce and applicants to the Customer. If such monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier shall review the operation of its relevant policies and take affirmative/positive action where appropriate. The Supplier shall impose on its Sub-Contractors obligations similar to those undertaken by it in this clause S10-2.4 and shall procure that those Sub-Contractors comply with such obligations.

S9-2.4.5 The Supplier shall provide such information as the Customer may from time to time request (including information requested to be provided by any Sub-Contractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses S10-2.4.1 to S10-2.4.5 of this Call-Off Agreement.

S9-2.5 Equality

S9-2.5.1 The Supplier shall, and shall procure that each Sub-contractor shall, in performing its/their obligations under this Call-Off Agreement (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

S9-2.5.2 The Supplier further acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier shall use all reasonable endeavours to assist (and to ensure that relevant Sub-Contractor assists) the Customer in relation to same.

S9-2.6 Health and Safety

S9-2.6.1 The Supplier shall promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Agreement. The Customer shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Agreement.

S9-2.6.2 While on the Customer premises, the Supplier shall comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

S9-2.6.3 The Supplier shall notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Agreement on the Customer premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

S9-2.6.4 The Supplier shall comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other

persons working on the Customer premises in the performance of its obligations under the Call-Off Agreement.

S9-2.6.5 The Supplier shall ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

S9-2.7 Criminal Damage

S9-2.7.1 The Supplier shall maintain such standards of vigilance and will take all such precautions as are advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 ("Compensation Order") or as may from time to time be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

S9-2.7.2 If during the Call-Off Agreement Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation pursuant to the provisions of the Compensation Order ("CDO Event") the following provisions of this clause S10-2.7 shall apply.

S9-2.7.3 The Supplier shall make (or shall procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as practicable after the CDO Event and shall pursue any such claim diligently and at its cost. If appropriate, the Customer shall also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the cost of the Customer and the Supplier shall (at no additional cost to the Customer) provide such assistance as the Customer reasonably requires with such appeal.

S9-2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 10a- Supplier's Solution for Digital Hosting

CQC reference CQC ICTC 558
CQC Digital Hosting

CLARIFICATION OF UNDERSTANDING

QUESTIONS & SUBMISSION DOCUMENT

THIS DOCUMENT IS TO BE COMPLETED BY THE ORGANISATION AND SUBMITTED TO THE CARE QUALITY COMMISSION

Closing date for submission of this document

4pm 11th January 2016

NAME OF ORGANISATION: Axis12 limited

To be returned to the Care Quality Commission using the Delta eSourcing Portal.

Care Quality Commission
CQC ICTC 558

Contents

1. COMPANY DETAILS

A1.	ORGANISATION DETAILS	
1.1	Please state the full name of the organisation submitting this clarification	
	Axis12 limited	
1.2	Please state the registered office address	
	Address: Unit 14, 6-18 Northampton Street, London Postcode: N1 2HY	
1.3	Please state the company registration number	
	07215135	
1.4	Please state the VAT registration number	
	997480160	
1.5	To the best of your knowledge, does any director or senior officer of your organisation have any personal or financial connection with any member or senior officer of the Care Quality Commission?	N O
	If yes, please provide details N/A	
A2.	**CONTACT DETAILS (for communications, correspondence and enquiries relating to this submission)**	
2.1	Please state the contact's name, and position within the organisation:	
	Name: Dave Stuart Position: Director	
2.2	Please state the contact's address:	
	Address: Unit 14, 6-18 Northampton Street, London Postcode: N1 2HY	
2.3	Please state the contact's telephone number:	
	+44 (0)845 519 5465	
2.4	Please state the contact's email address:	
	tenders@axistwelve.com	

2. RESPONSE TO CLARIFICATION OF UNDERSTANDING

Providers must provide response to the questions below, to describe how they will meet the requirements of the service.

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

Each question will be scored between 0 – 4, the technical questions will make up 75% of the total score and will be scored according to the above definitions.

Providers are required to respond to all of the questions below. Questions should be answered in full and should not refer to other documents or appendices unless stated in the question.

Question no.	Weighting	Question

1	0%	**Overview** Tenderers must provide a concise summary highlighting the key aspects of the proposal. (This response is not evaluated and should be used to contextualise the Tenderer's response, maximum 250 words) --- • Drupal hosting experts • BSI ISO27001 certified for over three years • Fully secure hosting facilities • Track record of meeting uptime/issue resolution targets • Established support processes/monitoring tools meet requirements • Implementation within CQC's timescales • Full familiarity with all of CQC's systems, reducing/removing on-boarding time/cost Axis12 specialises in hosting enterprise, Drupal-based websites for both public
		This implementation will be led by our experienced team and ongoing support provided by infrastructure experts. We offer one of the most secure hosting environments in Europe (certified by PCI DSS, HMG-CESG, G Cloud, ISO27001 standard, and NHS IGSoC approved) with a fully comprehensive UK-based BCM and disaster recover strategy. Our proposal eliminates migration and on-boarding costs by using the current infrastructure, which has a proven track record of meeting CQC's requirements of uptime, scalability and performance. We provide a range of comprehensive reporting, monitoring and deployment tools and have proven experience of working alongside other suppliers to resolve issues quickly for minimum service disruption. Our knowledge of he CQC platforms, integrations and underlying infrastructure means we're well placed to expedite the resolution of issues. Our transparent approach to designing and managing our hosting services, coupled with proactive and robust processes around incident and service management, ensure that we will provide an excellent service to CQC. Our proposal offers full implementation of environments by 5 February with no loss of service and minimal risks, alongside fully secure hosting, robust monitoring and maintenance, and tools that will allow CQC access to autonomous monitoring, reporting and code deployment.

2	25%	**Leadership and ability to deliver** Provide details of how the service will be delivered and transition managed. The Tender will be evaluated on: • Understanding of the requirements • Appropriate leadership in the delivery of the tender • Supplier's competency with technologies, track record, and demonstrated expertise • Has a defined and achievable timeline • Has identified and proposes suitable management of the delivery risks • Has a quality assurance regime that monitors, measures and assures quality outcomes Axis12 has several years' experience in hosting, developing and supporting CQC's digital sites and the integrations with CQC's enterprise systems. This allows us to fully understand the hosting requirements, particularly the high-profile nature of the service provided by the digital team. **Service delivery** Implementation of this proposal would be led by one of Axis12's directors, **Luke Harrop**, who has 20 years of IT consultancy experience, working with clients in the financial, telecommunications, publishing and government sectors. PRINCE2 qualified, he has specialist experience in cloud-based enterprise infrastructure, large-scale content management and publishing on demand systems. Luke has

managed the successful implementation of multiple hosting projects.

Working with other suppliers
Our experience of working with other suppliers (hosting/development/support suppliers) spans many high-profile websites, including High Speed Link 2 and the London Evening Standard.

We've found that where there are clear client-side processes around communicating, triaging and managing issues between multiple suppliers, problems are usually resolved more quickly.

Our hosting support time/costs reflect an expectation that there will be a higher requirement for liaison between suppliers in the first three months of the contract, with a slight reduction as the website support and hosting move more into business as usual. This liaison time will not be needed if the support and hosting is awarded to the same supplier.

Our technological expertise

We have proven expertise with the following technologies.

- Linux – Ubuntu 14.04
- Drupal – latest Version 7 or 8
- Varnish – HA caching/reverse proxy solution
- HA proxy - HA reverse proxy solution
- SNORT – Intrusion detection
- PHP – 5.6 and 7
- Apache – 3.2
- Apache SOLR search – 3.x – 5.x
- MySQL – 5.5 and above
- Mulesoft ESB – 3.7.0 CE
- GIT for version control – Bitbucket

Proven track record and client feedback

We provide hosting services for a number of high-profile clients, with a proven track record of infrastructure design, site uptime and good customer service.

Evidence - High Speed Link 2

HS2 launched their new website in January 2013, requiring a supplier who could provide a solid and robust hosting solution, as well as exceptional support to help host, manage and maintain the website. Axis12 have provided a robust hosting platform, managing the traffic to the site, as well as providing full stress and penetration testing.

Evidence - London Evening Standard
The Going Out site launched a robust, fast and responsive site successfully on time and to budget. Traffic has grown dramatically month-on-month and Axis12 continues to host and maintain the Evening Standard Going Out site.

Brian Alford, Digital Technology Manager said...
"Axis12 has been instrumental in architecting the entire stack to meet the demands of a high-traffic website and their extensive technical knowledge of enterprise-level servers and technologies has resulted in us having a well-structured stack that has been designed to meet our traffic demands. Our support tickets have been resolved promptly and their Sys Admins are willing to help explain technical challenges to us. I would have no hesitation in recommending Axis12 for hosting and support."

Evidence – Tate

Axis12 were tasked with providing consultancy aimed at the technical architecture, coming up with a way of modifying the existing hosting platform to be designed and configured to support the new Drupal CMS.

John Stack, Head of Tate Online said...
"In 2012 Tate re-launched its website as the culmination of a two-year project. Although Tate has a skilled in-house web development and information systems teams, the technologies that we selected were not ones that we had extensive experience of: Drupal, Varnish, Solr, High Scalable infrastructure, and a design strategy which would perform and look good on mobile devices. Furthermore the new website was to be launched on new hosting infrastructure. We therefore selected Axis 12 to help us design and implement a new hosting and technical architecture to deliver our ambitious project. They proved a more than capable partner in this complex endeavour and were on hand to make sure that we had a successful launch and to support the site in its early life. Since the launch we have now put in place an ongoing support arrangements that will see this partnership continue as the site is extended and developed in the years to come."

Timeline

There would be no lead time on the majority of the infrastructure because we propose to use existing infrastructure, CDN and reporting/monitoring tools would also be retained and available from 1 February 2016.

Environment build

Environment	CQC public site	Online communities	Provider portal
Production	1 Feb 2016	1 Feb 2016	1 Feb 2016
DR	1 Feb 2016	-	1 Feb 2016
Stage	-	-	1 Feb 2016
Test 1	1 Feb 2016	-	1 Feb 2016
Test 2	-	-	1 Feb 2016
Dev	5 Feb 2016*	5 Feb 2016*	1 Feb 2016

*There will be a small lead time for building the requested additional development environments (please note that they currently exist but for Axis12 use only – the lead time is to make them available for use by CQC and third-party suppliers).

Timeline for additional tasks

Task	Days	Earliest availability

		date (dependent on support supplier timelines)
Provide access to copy databases from Production to non-Production environments and vice versa	6 days	12 February 2016
Provide access to download databases and assets to create local dev environments	0.5 days	8 February 2016
Provide access to deploy code to all environments	1 day	9 February 2016

Delivery risks

Retention of existing infrastructure, integrations and service management processes will mean that migration risks are minimal.

Risk	Mitigation
Support supplier delays could risk implementation and delivery dates	- Engage with CQC and the support supplier to identify dependencies and align schedules at the beginning of the project - Identify a clear owner/point of contact at CQC so that all issues are triaged, allocated and tracked effectively, preferably in one system - Work closely with other suppliers to ensure all issues are resolved as efficiently as possible - Regular meetings to provide early sight of potential risks and issues, monitor progress and adjust timescales where necessary - If delays or timescales pose a significant risk to delivery, work with CQC to prioritise tasks to ensure most valuable are carried out first and anything that can be delivered post-transition is scheduled accordingly
There are changes or additional requirements from CQC	- Actively engage with CQC to understand the changes/new requirements - Work with CQC to understand and define priorities - Agree the deadlines for final specification and requirements - Define the minimal viable product for delivery to ensure that if anything is blocked or delayed, the delivery of the system is not affected.

Quality assurance processes

We ensure consistent quality in our delivery through the planning, setting and implementation of specific and measurable quality objectives. Our dedicated Account Manager, in consultation with your project team, will work together to produce quality objectives with associated milestones, which will then be constantly monitored throughout the delivery process.

We'll work with you to ensure that the responsibilities for managing service delivery are clear and appropriately allocated between CQC and the service suppliers. No matter which management methodology is applied, we prefer to ring-fence quality standards so they cannot be compromised.

		Finally, we recommend the use of a Service Level Agreement to ensure all parties are clear about responsibilities, key milestones, quality standards, testing procedures and ongoing service agreements. This helps to manage expectations and ensure value for money. ***Continuous Improvement*** We strive to be the best provider of open source web enterprise services in the industry and, therefore, ensure that everyone in Axis12 is accountable for fully satisfying our customers by meeting, or better yet exceeding, your needs and expectations with first-class solutions and services.
3	25%	**Technical Merit** Describe, with specific reference to the volumetric information, KPI's and requirements, the infrastructure design. The response will be evaluated on the; • Overall solution design • Expectation of meeting performance KPI's • Transparency of design including details on shared infrastructure **Meeting CQC's targets** Our current infrastructure design has a proven track record of meeting CQC's requirements.

Availability metric	Monthly target	Response
Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%	Our infrastructure design for CQC and other high-profile clients consistently meets 99.95% uptime targets
Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%	We provide a dedicated authoring web to allow us to add additional resources to the editing environment. This helps to minimise impact on the live environment and provide stability for authoring and admin tasks.
Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%	All planned maintenance is tested thoroughly across environments and implemented in non-business hours to cause minimum disruption to your service.
Non-Live environments to be available during standard business hours	99%	Up time for non-live environments consistently meet CQC's targets
Non-Live environments to be available outside standard business hours	95%	Most planned maintenance on non-live environments will be implemented in non-business

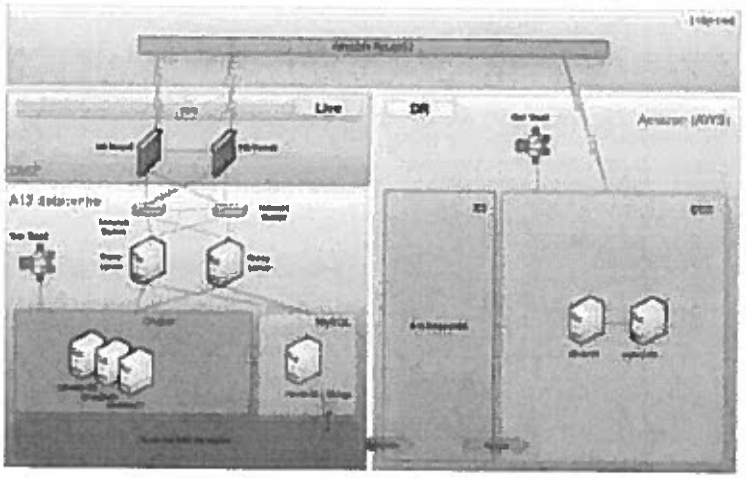
			hours. This will be planned with CQC to keep downtime to a minimum in non-core business hours
In the event of any compromise to the full service (e.g. in the case of invoking a disaster recovery service) the full service shall be restored within 12 hours		100%	Our response time for severity 1 issues is usually immediate. Working with the support supplier, a maintenance page should be displayed within minutes and complete failover, including DNS changes, will be complete within ~30 minutes. Once the root cause of the outage is resolved and the primary environment is stable, the site would be bought out of DR, the DB copied back and DNS repointed back to the original primary infrastructure.

Overall solution design

CQC public site

Component		Dev	Test	Prod (Live)	Prod (DR)
Security rating		IL0	IL0	IL0	IL0
Web	Drupal 7	1 unit	2 units	6 units	6 units
DB	MySQL	1 unit	1 unit	4 units	4 units
Caching	Varnish	Shared	Shared	Shared	Shared
Search	Solr	Y	Y	Y	Y
CDN	Edgecast	N	Y	Y	Y
Monitoring	New Relic	N	N	Y	Y
	Zenoss	Y	Y	Y	Y
SNORT	IDS	Y	Y	Y	N
DNS management	Route53	Y	Y	Y	Y
Self-management tools	Jenkins for deployment and Drush	Y	Y	Y	Y
	Access to New Relic reports	N	N	Y	Y

System diagram



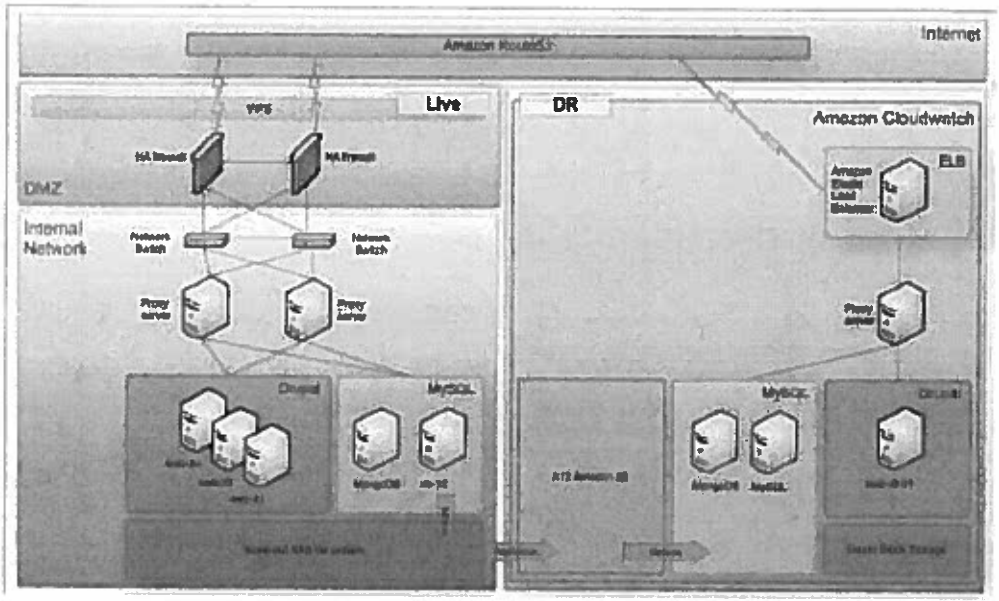
Online communities

Component		Development	Production (Live)
Security rating		IL2	IL2
Web	Drupal 7	1 unit	4 Units
DB	MySQL	1 unit	2 units
Caching	Varnish	Shared	Shared
Monitoring	New Relic	N	Y
	Zenoss	Y	Y
SNORT	IDS	Y	Y
DNS Management	Route53	Y	Y
Self-management tools	Jenkins for deployment and Drush	Y	Y
	Access to New Relic reports	N	Y

Provider Portal

Component		Dev	Test 1	Test 2	Stage	Prod (live)	Prod (DR)
Security rating		IL2	IL2	IL2	IL2	IL2	IL2
Web	Drupal 7	3 units	3 units	3 units	4 units	6 units	6 units
DB	MySQL	2 units	2 units	2 units	4 units	4 units	4 units
Caching	Varnish	Shared	Shared	Shared	Shared	Shared	Shared
Search	Solr	N	N	N	N	N	N
CDN	CloudFront	N	N	N	N	N	N
Monitoring	New Relic	N	N	N	N	Y	Y
	Zenoss	Y	Y	Y	Y	Y	Y
IDS	SNORT	Y	Y	Y	Y	Y	N
DNS	Management	Route5	Route5	Route5	Route5	Route5	Route5
		3	3	3	3	3	3
	Owner	Axis12	Axis12	Axis12	Axis12	Axis12	Axis12
Self management tools	Access to New Relic reports	N	N	N	N	Y	Y

System diagram



Our hosting facilities

To meet the requirements for the CQC infrastructure, especially the estimated user traffic and load for the Provider Portal and CQC public site, we propose that the primary site is hosted within our dedicated facilities housed at 'the Bunker' datacentre based in Kent, UK and the Disaster Recovery infrastructure be hosted in the Amazon cloud (AWS) EU Region.

In line with CQC's requirement for tier-3-equivalent hosting, the Bunker datacentre is certified by PCI DSS, HMG-CESG and G Cloud, is ISO27001 certified, and approved by NHS IGSoC. It provides one of the most secure hosting environments in Europe located within purpose-built, armoured, nuclear-bombproof, military-specified fortresses.

This level of security and redundancy is coupled with the ability to support high levels of power and cooling and stringent access control procedures. Our datacentre is staffed 24×7×365 by security, technical and networks staff able to provide remote hands or to be booked to carry out more complex tasks right up to full system builds.

The datacentre is linked to the Internet by our own fully redundant, multi-homed, gigabit network picking up multiple carriers from and number of POPS in locations in London, and offers the following features:

- Redundant air conditioning units to guarantee stable temperature and humidity @ N+1
- Redundant UPS conditioned power @ N+1
- Diverse Power Supplies with diesel generator back-up @ N+1
- Very Early Smoke Detection Apparatus installed and smoke detection

system
- Fire suppression system
- CCTV system
- 24-hour video recording
- Visual verification of all persons entering the data floor
- Guardroom (fitted with bullet-proof glass)
- Onsite security staff (ex-military & police)
- Random patrols with guard dogs
- Infrared cameras
- Vehicular gate with control barrier

Resilience is provided across our Priority 1 systems through load-balanced firewalls and switches, multiple reverse proxy servers with automatic failover capability, multiple high-availability webservers and a scale-out NAS file system.

Standard backups are stored on dedicated backup infrastructure, and are subject to our standard retention policies – daily backup with 7 generations. Backup logs are reviewed on a daily basis to avoid corruption.

All server and application configuration is version controlled and managed via automated configuration software, allowing us to redeploy at short notice. Code would be replicated across git repositories to ensure that the DR platform always had the latest code. Database dumps would be taken on a nightly schedule and transferred to DR where they will be hosted on Amazon's Glacier backup storage.

Amazon servers would be provided through standard on-demand instances. Varnish servers would be always on and configured to serve a custom page until DR is invoked. When DR is invoked, the latest backup would be restored to the DR database, and the webservers would be brought online. The DNS will be managed through Amazon route53 that would allow for a rapid repointing from Live to DR in the event of DR being invoked.

ISO27001 certification with BSI
We understand the importance of secure hosting and can fully meet CQC's requirements for IL2 hosting. We've been ISO27001 certified with the British Standards Institution (certification number 598644) for almost three years. We have a CLAS certified consultant who works with us regularly to ensure our processes meet the high standards of data security. We are familiar with HMG Security Policy Framework (Cabinet Office, October 2013; www.gov.uk/government/publications/security-policy-framework).

Our experience includes design, development and support of a number of IL2 certified systems, and the implementation and support of IL3 systems.

All of our processes and procedures incorporate Physical, Human and Digital security capability to ensure that client data and clients systems are continually secure against threats to Confidentiality, Integrity and Availability.

Axis12 employees undergo security screening and CRB checks, and are provided with solid training to ensure that the needs of our clients are managed and the aspirations of our workforce remain high. We guarantee security by only providing certain levels of access (such as server-level access) to suitably qualified and trained Axis12 staff (who are covered by ISO27001 certification) on an as-required basis.

Scaling capacity and performance

Our UK hosting is based on a combination of physical infrastructure based in a secure N+1 datacentre and cloud based hosting. This virtual hypervised architecture provides a scalable and fault-tolerant solution. The hypervised KVM layer uses the full range of hardware virtualisation support, and directly uses the regular Linux scheduler and I/O device drivers.

Provisioning of servers is automated with configuration management controlled by puppet. This allows us to scale the infrastructure quickly and efficiently using a set of version controlled 'recipes' that can be tailored to customer requirements where necessary.

All systems are load balanced to ensure there is no single point of failure.

We would work closely with CQC to plan for any upcoming events that might result in sharp increases in site traffic (e.g. publicity announcements, campaigns etc.). In these situations we are able to quickly upscale the hosting footprint to accommodate these demands, and then return them to the normal state once the event has past.

Business continuity and disaster recovery
Axis12 can offer CQC various packages for business continuity and disaster recovery. With our dual UK-based datacentres, we can offer a fully comprehensive BCM and disaster recovery strategy or, where appropriate or requested, we can utilise AWS (Amazon Web Services) to offer a secondary site as a warm standby.

We recommend the use of Route53 for DNS management, as this allows us reroute traffic to a secondary site faster, and commit to lower Recovery Time Objectives (RTO).

- **Recovery Time Objective:** standard as 30 mins from the point of DNS resolution.
- **Recovery Point Objective:** standard as 24 hours. This can be reduced as required by the introduction of intraday database backups.

Our most requested implementation for a DR site uses a primary site in one of our UK datacentres with a warm-standby hosted in either a separate UK-based datacentre or the cloud. Active/Active configurations are available on request.

Penetration testing
Axis12 engage third-party suppliers (most commonly NCC Group – (https://www.nccgroup.trust/uk/) to conduct penetration testing on our hosting infrastructure in order to identify potential security issues that could lead to the compromise or abuse of systems that could impact negatively on our client's business or reputation.

The tests used confirm that the infrastructure has been effectively hardened in line with best practice and provides the appropriate level of security.

Such testing typically includes:

- Network level scanning of all servers and network devices which make up the architecture
- Server build and configuration reviews of:
    - Proxy Servers
    - Web Servers
    - MySQL Servers
- MySQL Database Review
- Firewall rule set review

4	25%	**Service Management** Describe, with specific reference to the volumetric information, KPI's and requirements, the service design. The response will be evaluated on the; • Overall service design • Expectation of meeting service management KPI's • Transparency of service design including details of experience and qualifications of resource used to provide the service **Our hosting support services** ***Technical support team*** Overall account management will continue to be provided by **Luke Harrop** (who will be the route of escalation) with hosting support provided by our range of technical experts, including: • **Catherine Holland** - Catherine will be the main point of contact with CQC. She is an experienced account manager who will arrange and coordinate meetings with CQC, circulate monthly reports and ensure requests and issues are received, triaged, responded to and resolved according to our SLA. • **Dave Stuart** – an internationally renowned and highly respected technical expert on Internet technologies, who is often invited to speak at international events such as DrupalCon. He has worked with clients in music, broadcast media, education and legal sectors and for a number of public sector organisations. Dave provides technical leadership to our development team and heads up our research lab to drive technical innovation within Axis12. • **Pius Chungath** – an incredibly knowledgeable systems engineer and technology evangelist with a degree in computer science, a Masters degree in information security and 15 years' experience with numerous public- and private-sector clients. ***Support processes*** We track all support activity through a web-based system called Jira, but can also use our clients' preferred ticketing system. This allows us to provide you with total transparency over the way an issue is being handled and report on our activities against the service level agreement each month. We use the following process: 1. Client identifies an issue, or has a question. 2. Client raises a ticket usually via telephone (for Severity 1 issues) or email (for all other severities) 3. Tickets raised by email will automatically create a record in our ticketing system – within the 30 minute requirement by CQC 4. Axis12 review the ticket and begin diagnosis according to our SLA (immediately for Severity 1 issues) 5. The engineer updates the ticket regularly, which triggers an automated email to the client. In this manner, the client is aware of all activity on the ticket. In the case of Severity 1 issues, an action plan is likely to be formulated as soon as the call is logged and regular conference calls scheduled until issue is fixed. 6. Once the client is happy that the issue is resolved, the system is updated

as completed and the person who logged the ticket is automatically alerted via email. his is to ensure that tickets aren't closed without the person who logged the ticket knowing about it.

Service level agreement

Issues are categorised into severity levels as per the potential and/or real impact they have on the normal operation of the production site. Our response and typical resolution times fall well within CQC's requirements.

- **Severity 1** – an issue that results in the loss of a facility or function material to the proper operation of the systems.
- **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.
- **Severity 3** – an issue that affects a small number of users but does not prevent business critical activity.
- **Severity 4** – an issue that affects how users perform tasks but workarounds are available.

Level	Supplier will respond to issues raised, and commence investigation	Resolution targets*
Severity 1	Usually immediate with a call back	Within 1 hour(s) of investigation commencing**
Severity 2	2 hours	Within 5 hours of investigation commencing
Severity 3	5 hours	Within 2 business days of investigation commencing
Severity 4	24 hours	Within 5 business days of investigation commencing

*Where issues are between hosting and support or the root cause is unclear, we'll work closely with the support supplier to ensure that CQC receives the fastest possible resolution. However, this may mean that we're unable to meet our targets where the failure is outside of our sphere of influence.

**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.

Service requests

Service requests will be impact assessed within three days and timescales/SLAs for implementation agreed with CQC and monitored through regular communication and our Jira tracking system.

Support requests outside of the base contract

We can provide additional support, as required, at the costs illustrated below. This may be required for major upgrades (e.g. OS or PHP upgrades) and can be discussed as required.

RATE CARD

Role	Daily Rate
System administration	£650
Support development (e.g. fixing defects/inefficiencies, configuration tasks)	£650
Feature development (e.g. development of new features/additions to existing features)	£850

		Technical/Solutions Architect	£850
		Project Management/Scrum Master	£850

All prices are ex VAT and do not include expenses

Monthly service report

Our monthly client reports typically include the following, but we are happy to customise them to your requirements.

- A summary of activity for the period – including incident reports, action points and progress/resolution, current service requests and progress, and release schedules/progress
- A list of all incidents (and a copy of the relevant incident report) for the period
- A list of all support tickets worked on for the period
- A copy of availability and performance graphs for each production server for the period

The monthly report will be circulated to the required list of people according to CQC's timescales.

Maintenance

Monitoring

We will constantly monitor your service to collect and track metrics, gain insight, and react immediately to keep your applications and businesses running smoothly. We can also monitor against custom metrics generated by a customer's applications and services, if required.

We use the following tools for monitoring and reporting:

- **Pingdom** – is provided to our clients as a standard and impartial check of request response time to predefined URLs. This can be configured to send notifications by email or SMS to a predefined list of people.
- **New Relic** – is a SaaS based product that Axis12 use extensively to monitor if any servers have capacity issues so you can take corrective action, CPU utilization, memory utilization, disk I/O utilization, and disk capacity. It allows us to follow the performance of critical transaction across the entire service-oriented application environment; provides code-level visibility and the ability to drill down to see the performance impact of specific code segments and SQL statements; and gain deeper insight into a key transaction's performance by showing transaction traces alongside long-running profiler results.
- **Zenoss** - provides a web interface that allows us to monitor availability, inventory/configuration, performance, and events. Zenoss is configured to notify our support team by email and SMS before issues are encountered by monitoring resource consumptions thresholds and pattern matching on key web assets.

Administration

Standard backups are stored on dedicated backup infrastructure, and are subject to our standard retention policies – daily backup with seven generations. Backup logs are reviewed on a daily basis to ensure they are not corrupted. Restoration of backups is not included in the base maintenance contract but support for this can be requested through our online ticketing system.

We use Jenkins for orchestrating Continuous Integration in the dev environment, and for deploying code to production sites. We can provide secure access to our clients (or clients' suppliers) to enable them to manage their own releases directly out of the Git repo.

Performance testing
Our infrastructure allows for meaningful performance testing before new code is released into the production environment. Where needed, we can support you in designing, implementing and reporting on performance testing. Please see rate card for rates.

Secure administration access
Where a high level of editorial activity is anticipated, Axis12 would always recommend the use of a dedicated Authoring web that is not exposed to public users and is enabled with Apache Authentication of additional security. This allows us to provide additional resources to the editing environment, and minimises any impact to site performance that heavy editorial activities might cause.

Patching and upgrades
Axis12 maintain a strict maintenance cycle for OS security updates and patching. Our dev/test servers receive all patches via our local Aptcacher server. These patches are tested by our support staff prior to deployment to production environments and will be deployed out of hours to cause minimum disruption to your service.

Please note that major upgrades, e.g. upgrades to PHP versions or OS upgrades, will need to be discussed with CQC and in conjunction with the application support team - as they will typically constitute a significant amount of work outside of the base hosting contract.

Schedule 10b- Supplier's Solution for Digital Hosting Managed Service

Care Quality Commission

CQC reference CQC ICTC 554
CQC Digital Hosting Managed Service

CLARIFICATION OF UNDERSTANDING

QUESTIONS & SUBMISSION DOCUMENT

THIS DOCUMENT IS TO BE COMPLETED BY THE ORGANISATION AND SUBMITTED TO THE CARE QUALITY COMMISSION

Closing date for submission of this document

4pm 11th January 2016

NAME OF ORGANISATION: Axis12 Limited

To be returned to the Care Quality Commission using the Delta eSourcing Portal.

Contents

1. COMPANY DETAILS

A1.	ORGANISATION DETAILS	
1.1	Please state the full name of the organisation submitting this clarification	
	Axis12 limited	
1.2	Please state the registered office address	
	Address: Unit 14, 6-18 Northampton Street, London, N1 2HY Postcode: N1 2HY	
1.3	Please state the company registration number	
	07215135	
1.4	Please state the VAT registration number	
	997480160	
1.5	To the best of your knowledge, does any director or senior officer of your organisation have any personal or financial connection with any member or senior officer of the Care Quality Commission?	NO
	If yes, please provide details N/A	
A2.	**CONTACT DETAILS (for communications, correspondence and enquiries relating to this submission)**	
2.1	Please state the contact's name, and position within the organisation:	
	Name: Dave Stuart Position: Director	
2.2	Please state the contact's address:	
	Address: Unit 14, 6-18 Northampton Street, London Postcode: N1 2HY	
2.3	Please state the contact's telephone number:	
	+44 (0)845 519 5465	
2.4	Please state the contact's email address:	
	tenders@axistwelve.com	

2. RESPONSE TO CLARIFICATION OF UNDERSTANDING

Providers must provide response to the questions below, to describe how they will meet the requirements of the service.

Each question will be scored between 0 – 4, the technical questions will make up 65% of the total score and will be scored according to the below definitions.

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

Providers are required to respond to all of the questions below. Questions should be answered in full and should not refer to other documents or appendices unless stated in the question.

Question no.	Weighting	Question
1	0%	**Overview** Tenderers must provide a concise summary highlighting the key aspects of the proposal. (This response is not evaluated and should be used to contextualise the Tenderer's response, maximum 250 words) • Drupal experts • BSI ISO27001 certified for over three years • Experience of supporting IL2 systems • Track record of meeting CQC's uptime/issue resolution targets • Established support processes/monitoring tools meet CQC's requirements • Implementation within CQC's timescales • Full familiarity with all of CQC's systems reducing/removing on-boarding time/cost

		Axis12 specialises in supporting enterprise, Drupal-based websites for both the public and private sector. This implementation will be led by our experienced team and ongoing support will be provided by Drupal experts. We've been BSI ISO27001 certified for almost three years and have a proven track record of supporting IL2 systems. Our familiarity with the CQC systems eliminates the cost and time for handover/health check and our proposal is largely based on the use of current monitoring, deployment and support systems and processes, which have a proven track record in meeting most of CQC's requirements of uptime, problem management and service management. We propose to provide a range of comprehensive reporting, monitoring and deployment tools and have proven experience of working alongside hosting-only suppliers to resolve issues quickly for minimum service disruption. Our knowledge of Drupal, the CQC platforms and their integrations mean we are well placed to expedite the resolution of issues if they arise. We propose to support the site as-is, with no changes to modules, code or functionality. Retention of existing caching and monitoring will help to ensure site stability. Additional requested features will be implemented by 1 March 2016 to enable CQC to manage the software more autonomously.
2	25%	**Leadership and ability to deliver** Provide details of how the service will be delivered and transition managed. The Tender will be evaluated on: • Understanding of the requirements • Appropriate leadership in the delivery of the tender • Supplier's competency with technologies, track record, and demonstrated expertise • Has a defined and achievable timeline • Has identified and proposes suitable management of the delivery risks • Has a quality assurance regime that monitors, measures and assures quality outcomes Axis12 has several years of experience in hosting, developing and supporting CQC's digital sites and their integrations with CQC's enterprise systems. This allows us to fully understand the support requirements, particularly the high-profile nature of the service provided by the digital team. Our experience of supporting the current systems means that we understand and have a proven track record of meeting CQC's requirements and KPIs. **Service delivery** Implementation of this proposal would be led by one of Axis12's directors, **Luke Harrop**, who has 20 years of IT consultancy experience, working with clients in the financial, telecommunications, publishing and government sectors. PRINCE2 qualified, he has specialist experience in cloud-based enterprise infrastructure, large-scale content management and publishing on demand systems. Luke has

managed the successful implementation of multiple support projects.

Working with other suppliers
Our experience of working with other suppliers (hosting/development/support suppliers) spans many high-profile websites, including High Speed Link 2 and the London Evening Standard.

We've found that where there are clear client-side processes around communicating, triaging and managing issues between multiple suppliers, problems are usually resolved more quickly.

Our expectation is that there will be a higher requirement for liaison between suppliers in the first three months of the contract when the site is migrated to new infrastructure, with a slight reduction as the website support and hosting move more into business as usual. This time would come from the ad hoc allocation of 12 days per month. This liaison time will not be needed if the support and hosting is awarded to the same supplier, but there is likely to be additional time needed to liaise with development staff.

Our technological expertise
We have proven expertise with the following technologies.

- Linux – Ubuntu 14.04
- Drupal – latest Version 7 or 8
- Varnish – HA caching/reverse proxy solution
- HA proxy - HA reverse proxy solution
- SNORT – Intrusion detection
- PHP – 5.6 and 7
- Apache – 3.2
- Apache SOLR search – 3.x – 5.x
- MySQL – 5.5 and above
- Mulesoft ESB – 3.7.0 CE
- GIT for version control – Bitbucket

Penetration testing
Axis12 engage third-party suppliers (most commonly NCC Group – (https://www.nccgroup.trust/uk/) to conduct security testing of client applications to:

- Expose weaknesses stemming from the application's relationship to the rest of the IT infrastructure
- Assess application security versus real-world attacks via a variety of manual techniques
- Identify security design flaws
- Increase end-user confidence in the application's overall security

Industry-standard penetration testing is estimated at £3000 per platform, as costed by NCC for a two-day test. Any rectifications required after the initial test will need to be billed separately.

If Axis12 won both the hosting and support contracts, application penetration testing would not be required because it has already been carried out with the current application/infrastructure combination.

Proven track record and client feedback
We provide support services for a number of high-profile clients, with a proven track record of robust infrastructure, monitoring, reporting, issue resolution and good customer service.

Evidence - High Speed Link 2
HS2 launched their new website in January 2013, requiring a supplier who could provide exceptional support to manage and maintain the website. Interest in HS2 continues to grow and, as the project continues to progress, the website is receiving several thousand more hits per month, as well as users continuously downloading much of the same content (e.g. very detailed and large-scale maps and plans).

Axis12 were tasked with managing the traffic to the site, as well as providing full stress and penetration testing. As we are experts in Drupal 7, our experience and specialist knowledge came to great effect in removing nuances and managing any issues quickly and efficiently, usually in a pre-emptive manner.

Evidence - London Evening Standard
The Going Out site launched a robust, fast and responsive site successfully on time and to budget. Traffic has grown dramatically month-on-month and Axis12 continues to host and maintain the Evening Standard Going Out site.

Brain Alford, Digital Technology Manager said...
"We are very extremely happy with the Evening Standard website project that Axis12 carried out for us and which they continue to provide support and hosting for. Luke Harrop and Al Croston have both been very helpful in responding to our queries and working with us to create a stable site. Our support tickets have been resolved promptly and their Sys Admins are willing to help explain technical challenges to us. I would have no hesitation in recommending Axis12 for web design, application development, hosting and support."

Evidence - Tate
In early 2011 the Tate Group embarked on an ambitious project to migrate their flagship Tate Online web presence over to a Drupal platform. Unusually, the site had to be accommodated on pre-existing hardware and a hosting platform originally designed for a different CMS.

Axis12 were tasked with providing consultancy aimed at building and supporting the site on new architecture and now support the new Tate Online platform.

John Stack, Head of Tate Online said...
"In 2012 Tate re-launched its website as the culmination of a two-year project. Although Tate has a skilled in-house web development and information systems teams, the technologies that we selected were not ones that we had extensive experience of: Drupal, Varnish, Solr and High Scalable infrastructure. We therefore selected Axis 12 to help us design and implement a new hosting and technical architecture to deliver our ambitious project. They proved a more than capable partner in this complex endeavour and were on hand to make sure that we had a successful launch and to support the site in its early life. Since the launch we have now put in place an ongoing support arrangement that will see this partnership continue as the site is extended and developed in the years to come."

Timeline
Current support processes and issue tracking would be retained with no lead time. Implementing support features, such as monitoring, patching, configuring deployment tools, etc. would be largely dependent on the migration timelines provided by the hosting supplier.

If Axis 12 won both contracts, all existing support would have no lead time with a small amount of time required to configure and implement additional tools.

Additional hosting requirements

We believe that the following requirements would need to be implemented by the hosting supplier, but the support supplier would need to work with them on the implementation:

- Provide access to copy databases from Production to non-Production environments and vice versa
- Provide access to download databases and assets to create a local dev environment
- Provide access to deploy code to all environments

Timeline for system testing and additional features

	Days	Implementation dates (dependent on hosting timelines)
System and integration testing for transition*		
CQC Public Site testing: • CDN/application caching** • Elastic Email • Axis12 Find (SOLR) • ESB • Google Maps • Google Places • Google Geocode • Checkbox • DBs	10 days	16/02 - 29/02
Provider Portal testing: • ESB • DBs • OpenAM	10 days	16/02 - 29/02
Online Communities testing: • Elastic Email • DBs	4 days	22/02 - 25/02
Application penetration testing		
CQC public site	2 days	15/02 - 16/02
Provider Portal	2 days	15/02 - 16/02
Online Communities	2 days	15/02 - 16/02
Maintenance/deployment tools		
Ability to copy databases from Production to non-Production environments and vice versa***	Hosting contract. May require some configuration/testing under the support contract 0.5 day	22/02
Ability to download databases and assets to create local dev environments***	Hosting contract. May require some configuration/testing under the support contract 0.5 day	23/02

Access to all code repositories and branches	0.5 days	24/02
Ability to deploy code to all environments***	Hosting contract. May require some configuration/testing under the support contract 0.5 day	25/02

*System and integration testing will require significant testing resource from CQC and also availability and resource from the ESB supplier.
**Our proposal assumes that CQC's current arrangement of procuring licenses directly from EdgeCast and Google will remain. If this is not the case, please let us know.
***Our proposal assumes that the support supplier, rather than the hosting supplier, will configure and test the additional deployment tools. The time and cost (£975) for this can be removed if this is not the case.

Delivery risks

Risk	Mitigation
Delays in hosting migration could risk implementation and delivery dates	- Engage with CQC and the hosting supplier to identify dependencies and align schedules at the beginning of the project - Identify a clear owner/point of contact at CQC so that all issues are triaged, allocated and tracked effectively, preferably in one system - Work closely with other suppliers to ensure all issues are resolved as efficiently as possible - Regular meetings to provide early sight of potential risks and issues, monitor progress and adjust timescales where necessary - If delays or timescales pose a significant risk to delivery, work with CQC to prioritise tasks to ensure most valuable are carried out first and anything that can be delivered post-transition is scheduled accordingly
CQC resource required for system and integration testing is not available	- Early sight of detailed testing plans to agree resource requirements against availability - Identify a clear owner/point of contact at CQC so that all issues are triaged, allocated and tracked effectively, preferably in one ticketing system - Regular meetings to provide early sight of potential risks and issues, monitor progress and adjust timescales where necessary - If delays or timescales pose a significant risk to delivery, work with CQC to prioritise testing to ensure most valuable are carried out first and anything that can be delivered post-transition is scheduled accordingly
There are changes or additional requirements from CQC	- Actively engage with CQC to understand the changes/new requirements - Work with CQC to understand and define priorities - Agree the deadlines for final specification and requirements - Define the minimal viable product for delivery to ensure that if anything is blocked or delayed, the delivery of the system is not affected.

Quality assurance processes
We ensure consistent quality in our delivery through the planning, setting and implementation of specific and measurable quality objectives. Our dedicated

		Account Manager, in consultation with your project team, will work together to produce quality objectives with associated milestones, which will then be constantly monitored throughout the delivery process. We'll work with you to ensure that the responsibilities for managing service delivery are clear and appropriately allocated between CQC and the service suppliers. No matter which management methodology is applied, we prefer to ring-fence quality standards so they cannot be compromised. Finally, we recommend the use of a Service Level Agreement to ensure all parties are clear about responsibilities, key milestones, quality standards, testing procedures and ongoing service agreements. This helps to manage expectations and ensure value for money. ***Continuous Improvement*** We strive to be the best provider of open source web enterprise services in the industry and, therefore, ensure that everyone in Axis12 is accountable for fully satisfying our customers by meeting, or better yet exceeding, your needs and expectations with first-class solutions and services.
3	40%	**Service Management and Support** Describe, with specific reference to the volumetric information, KPI's and requirements, the service design. The response will be evaluated on: • Overall service design • Expectation of meeting service management and support KPI's • Transparency of service design including details of experience and qualifications of resource used to provide the service _____ **Overall service design** ***Application support team*** Account management will continue to be provided by **Luke Harrop** (who will be the escalation route) with additional account and technical support provided by: • **Catherine Holland** - Catherine provides our first-line of support and will be the main point of contact with CQC. She is an experienced account manager who will arrange and coordinate meetings with CQC, circulate monthly reports and ensure requests and issues are received, triaged, responded to and resolved according to our SLA. • **Dave Stuart** – an internationally renowned and highly respected technical expert on Internet technologies, who is often invited to speak at international events such as DrupalCon and specialist SOLR events. He has worked with clients in music, broadcast media, education and legal sectors and for a number of public sector organisations. Dave provides technical leadership to our development team and heads up our research lab to drive technical innovation within Axis12.

		• **Ed Brown** (Technical Architect, BSc) – with many years' experience developing robust and scalable Drupal solutions, Ed is a key member of the Axis12 team and is involved in projects from specification through to implementation (including the Provider Portal and CQC's public site). Ed has worked with Drupal for over 10 years and particularly enjoys supporting and developing high-traffic sites that provide a responsive and engaging experience for users. • **Demi Dimitropoulou** (Senior Developer) – with a keen interest of Drupal, and the web community in general, Demi has widespread knowledge of her area of expertise that helps us go above and beyond client expectations. Being the senior developer for the Online Communities platform, she he has a unique understanding of the system that will help to resolve issue quickly. ***ISO27001 certification with BSI*** We understand the importance of secure hosting and can fully meet CQC's requirements for IL2 hosting. We've been ISO27001 certified with the British Standards Institution (certification number 598644) for almost three years. We have a CLAS certified consultant who works with us regularly to ensure our processes meet the high standards of data security. We are familiar with HMG Security Policy Framework (Cabinet Office, October 2013; www.gov.uk/government/publications/security-policy-framework). Our experience includes design, development and support of a number of IL2 certified systems, and the implementation and support of IL3 systems. All of our processes and procedures incorporate Physical, Human and Digital security capability to ensure that client data and clients systems are continually secure against threats to Confidentiality, Integrity and Availability. Axis12 employees undergo security screening and CRB checks, and are provided with solid training to ensure that the needs of our clients are managed and the aspirations of our workforce remain high. We guarantee security by only providing certain levels of access to suitably qualified and trained Axis12 staff (who are covered by ISO27001 certification) on an as-required basis. ***Support process*** We track all support activity through a web-based system called Jira, but can also use our clients' preferred ticketing system. This allows us to provide you with total transparency over the way an issue is being handled and report on our activities against the service level agreement each month. We use the following process: 1. Client identifies an issue, or has a question. 2. Client raises a ticket usually via telephone (for Severity 1 issues) or email (for all other severities) 3. Tickets raised by email will automatically create a record in our ticketing system – within the 30 minute requirement by CQC 4. Axis12 review the ticket and begin diagnosis according to our SLA (immediately for Severity 1 issues) 5. The developer updates the ticket regularly, which triggers an automated email to the client. In this manner, the client is aware of all activity on the ticket. In the case of Severity 1 issues, an action plan is likely to be formulated as soon as the call is logged and regular conference calls scheduled until issue is fixed. 6. Once the client is happy that the issue is resolved, the system is updated

as completed and the person who logged the ticket is automatically alerted via email. In this manner, tickets can never be erroneously closed without the person who logged the ticket knowing about it.

Service level agreement

Issues are categorised into severity levels as per the potential and/or real impact they have on the normal operation of the production site. Our response and typical resolution times fall well within CQC's requirements.

- **Severity 1** – an issue that results in the loss of a facility or function material to the proper operation of the systems.
- **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.
- **Severity 3** – an issue that affects a small number of users but does not prevent business critical activity.
- **Severity 4** – an issue that affects how users perform tasks but workarounds are available.

Level	Supplier will respond to issues raised, and commence investigation	Resolution targets*
Severity 1	Usually immediate with a call back	Within 1 hour(s) of investigation commencing
Severity 2	2 hours	Within 5 hours of investigation commencing
Severity 3	5 hours	Within 2 business days of investigation commencing
Severity 4	24 hours	Within 5 business days of investigation commencing

*Where issues are between hosting and support or the root cause is unclear, we'll work closely with the hosting supplier to ensure that CQC receives the fastest possible resolution. However, this may mean that we're unable to meet our targets where the failure is outside of our sphere of influence.

Monthly service report

Our monthly client reports typically include the following, but we are happy to customise them to your requirements.

- A summary of activity for the period – including incident reports, action points and progress/resolution, current service requests and progress, and release schedules/progress
- A list of all incidents (and a copy of the relevant incident report) for the period
- A list of all support tickets worked on for the period
- A copy of availability and performance graphs for each production server for the period

The monthly report will be circulated to the required list of people according to CQC's timescales.

Additional resource outside of the support contract

We can offer additional support or development for requirements that fall outside of the support contract, at the following rates.

RATE CARD

Role	Daily Rate
System administration	£650

Support development (e.g. defects, inefficiencies, configuration tasks)	£650
Feature development (e.g. development of new features/additions to existing features)	£850
Technical/Solutions Architect	£850
Project Management/Scrum Master	£850

All prices are ex VAT and do not include expenses

Meeting availability requirements

Availability metric	Monthly target	Response
Live environments and data - the service utilised by an End User, i.e. citizen or a business including all data	99.95%	While largely dependent on the hosting infrastructure, our expertise of the Drupal platform allows us to provide support for CQC and other high-profile clients to ensure they consistently meet CQC's uptime targets
Contributed Environment and data - the service used by editors, developers in order to manage Content and/or transactions	99.8%	While largely dependent on the hosting infrastructure, our expertise of the Drupal platform allows us to provide support for CQC and other high-profile clients to consistently meet CQC's uptime targets
Planned maintenance and releases to the solution shall be completed outside of UK business hours and without disruption to the users	99.8%	All planned maintenance (patching, etc) is tested thoroughly across environments and implemented in non-business hours to cause minimum disruption to your service.
Non-Live environments to be available during standard business hours	99%	While largely dependent on the hosting infrastructure, our expertise of the Drupal platform allows us to provide support for CQC and other high-profile clients to consistently meet CQC's uptime targets
Non-Live environments to be available outside standard business hours	95%	Most planned maintenance on non-live environments will be implemented in non-business hours. This will be planned to keep downtime to a minimum in non- core business hours
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%	Our response time for a severity 1 issue is usually immediate. A maintenance page can be displayed within minutes and we will work with CQC and other suppliers to resolve the issue as quickly as possible to make the primary environment stable.

Maintenance

Patching and upgrades

Axis12 maintain a strict maintenance cycle for Drupal platforms, monitoring

module notifications throughout the month. Security and functional module patching is included in the 9 days of support per month. Where patching is significant or potentially disruptive, this will be scheduled with CQC.

We implement robust testing across environments for patching to ensure issues are not released to your live environment and will schedule releases to ensure minimum disruption to CQC's service. Typically, patches are released outside of business hours.

Monitoring
CQC's monitoring requirements can be achieved with New Relic. Our proposal assumed that New Relic will be implemented by the hosting provider but we will provide support to you to configure the software to meet your needs.

Backups

Backup and restore services are generally part of the hosting contract, but we are happy to provide this service as part of the support, if required.

Our standard backups are stored on dedicated backup infrastructure, and are subject to our standard retention policies – daily backup with 7 generations. Backup logs would be reviewed on a daily basis to ensure they are not corrupted.

SSH access
SSH access to the server is typically controlled and provided by the hosting supplier but we would work with them to negotiate this access on CQC's behalf.

Major upgrades

Please note that major upgrades, e.g. upgrades to PHP versions or major Drupal versions, will need to be discussed with CQC and in conjunction with the hosting supplier, as they will typically constitute a significant amount of work that may fall outside of the planned and ad hoc support days.

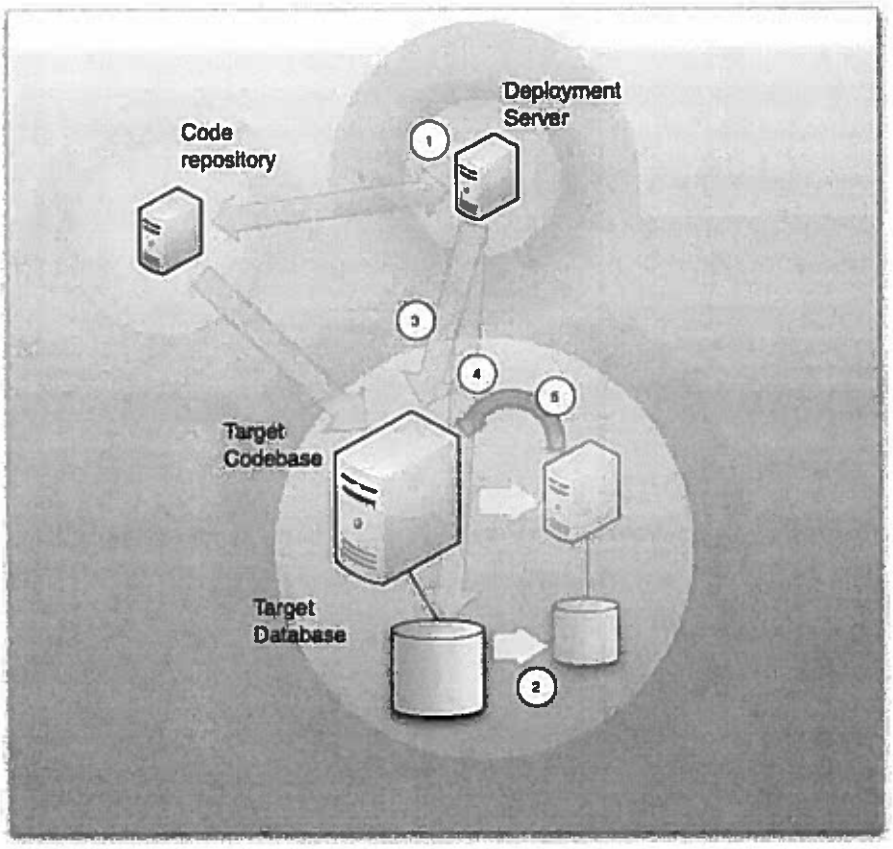
Deployment
Some of the deployment tools will need to be provided by the hosting supplier but we can provide support to configure them, schedule jobs and create deployment scripts.

We can supply deployment support both within and outside of business hours. We understand the importance of planning deployments to cause minimum disruption. Where deployment support is required outside business hours, a support request should be raised at least one week in advance to allow us to plan resource.

Our recommended deployment process
- The Deployment Server (Jenkins) initiates a release. Where changes are being applied to the development environment, the changes are deployed as immediately as possible either by Jenkins detecting a code commit or a scheduled cron job. In the case of other environments, the release manager usually triggers the initiation through the GUI.
- The Deployment Server (Jenkins) orchestrates a task, which backs up

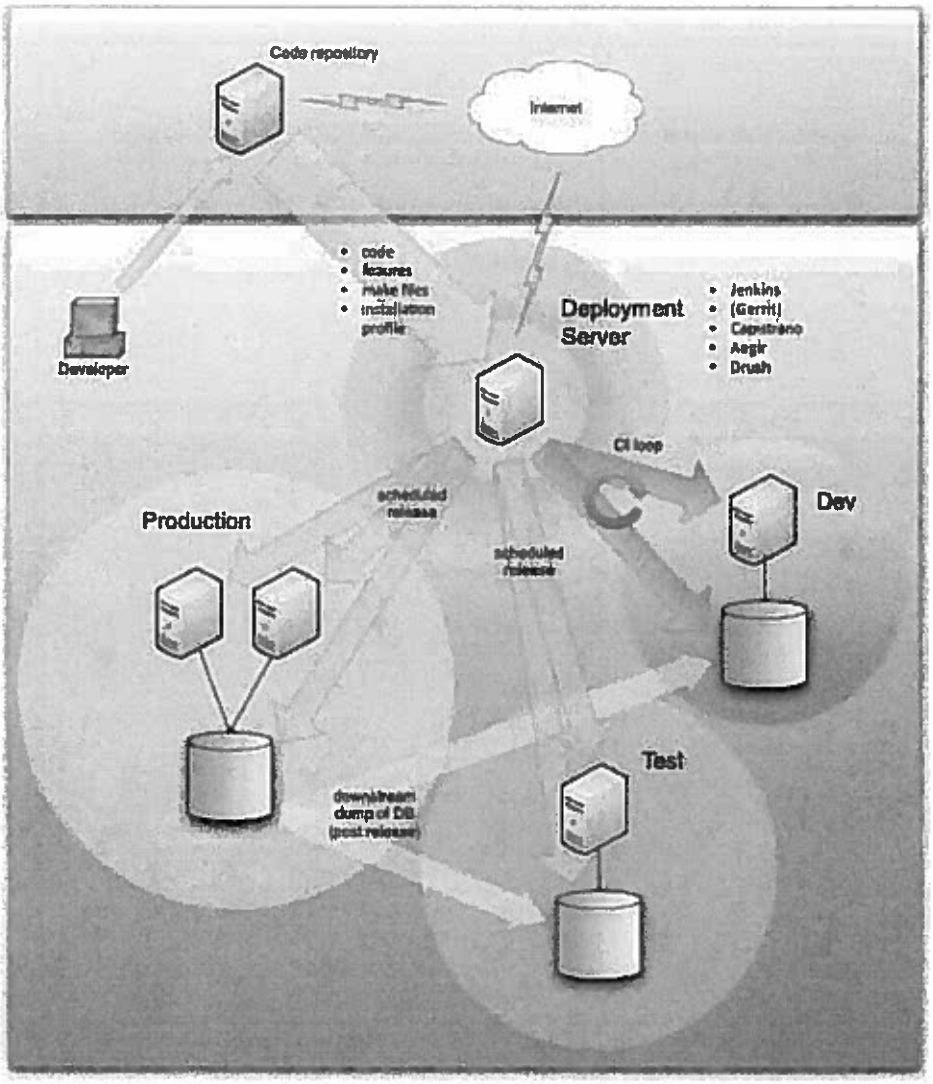
and dumps the existing database.

- The Deployment Server (Aegir) creates a new document root and checks out the entire codebase. This task is repeated for each of the webs within the system architecture.
- The Deployment Server (Aegir) runs through the make.file to apply changes to the database. Where the configuration changes are not fully automated in this way, database updates will be applied via either Selenium scripts and/or documented manual procedures.
- If all the previous steps are implemented successfully, the deployment Server (Aegir) drops the existing symlink to the document root and creates a new one that points to the updated codebase.



The deployment environment

The core of the deployment framework environment is the centralised deployment server, which provides the integration layer across the application estate and orchestrates all the deployment events. The deployment process is consistent across all of the application environments, thereby establishing maximum confidence in a release candidate before it is exposed to production.



Deployment tools and components

Code Repository

Code can be managed using a number of enterprise repository solutions (GIT, Bazaar, Subversion) which could be local to CQC's network, hosted on the hosting supplier's infrastructure, or implemented as a cloud solution such as GitHub. Axis12 recommends the use of Git as the repository of choice due to its inherent stability and comprehensive feature set.

Code checkouts and commits can be made over either ssh, http or https. Where distributed teams are involved, ssh is recommended for stability reasons.

Jenkins

Jenkins provides continuous integration services which runs in a servlet container such as Apache Tomcat. It supports SCM tools including CVS, Subversion, Git, Mercurial and Clearcase, and can execute Apache Ant and Apache Maven based projects as well as arbitrary shell scripts and Windows batch commands.

Builds can be started by various means, including being triggered by commit in a version control system, scheduling via a cron-like mechanism, sequencing (building when other builds have completed), or by requesting a specific build URL.

Gerrit
Gerrit is a web interface that integrates with Git. Gerrit will also provide secure access to the Git repository through the use of private/public keys and ssh/http username/passwords. If GitHub is being used, then Gerrit is not required as GitHub has its own interface.

Capistrano
Capistrano is used to run scripts across multiple servers. It automates the process of making a new version of an application available on one or more web servers, including supporting tasks such as changing databases.

Capistrano is written in the Ruby language and is distributed using the Ruby Gems distribution channel. It is an outgrowth of the Ruby on Rails web application framework, but has also been used to deploy web applications written using other frameworks, including ones written in PHP.

Capistrano is implemented primarily for use on the bash command line. Users may choose from many Capistrano 'recipes', (e.g. to deploy current changes to the web application or roll back to the previous deployment state).

Aegir
Aegir is a distributed instance management system designed to simplify the deployment and management of Drupal web sites. Aegir is built atop a standard LAMP stack, as well as Drush, a command line shell and Unix scripting interface for Drupal. It extends Drush with various provisioning functions, as well as providing a Drupal-based front-end control-panel.

In addition to the GUI interface, Aegir can be accessed via the command line or an API, which enables the automation of many website-related system administration processes. Being based on Drupal and Drush, Aegir is highly extensible, and several contributed modules exist to extend its functionality.

Drush
Drush allows you to control many common Drupal site administration tasks from your server's command-line. Some of the tasks that Drush can help you carry out more quickly from the command line include:

- Downloading new contributed modules
- Enabling and disabling modules
- Updating core Drupal code and modules
- Clearing Drupal caches
- Triggering the Drupal cron job

Performance testing
We can support you in designing, implementing and reporting on performance testing as part of your ad hoc support days.

Schedule 10c- Supplier's Additional Response

CQ1 Managed Service: Please can you clarify how you will ensure service continuity if key staff and personnel are unavailable?

Response

All applications are supported by both our dev and support teams. Within each team we have multiple individuals working on the applications, which provides a level of redundancy across the skills and experience required to support them. Furthermore, we have an internal knowledge-sharing programme to ensure that no one-key individual is responsible for any particular area and we ensure that, in the planning of holidays and staff absences, the appropriate level of support is not compromised.

CQ2 Managed Service Commercial: 'Other' tab items 3-6: CQC understand that the functionality that Axis 12 is proposing to build and configure already exists, therefore this will not be required and the costs should reflect this. Please can you clarify?

Response

This functionality exists for the public site only - the latest DB backup from live to test. This will need to be extended for the public site to meet your requirement then the same functionality implemented for both the Provider Portal and the Online Communities site. The cost covers the work required to do that.

CQ3 Digital Hosting: Please clarify how you will ensure the platform will remain fit for purpose in response to external changes and developments?

Response

With every new project or body of work that introduces functional change to the system, we would expect the managed service supplier to assess the risk to performance as part of their activities and plan for an adequate level of performance testing within the project, where deemed necessary.

As hosting supplier, we would expect to be made aware of any perceived risk associated with feature change in order to allow us to work with the managed service supplier in support of their testing and make recommendations around infrastructure change, should it be required.

CQ4 Managed Service: Please can you provide details around the cost of New Relic licenses? In your submission this is costed at a total of £13,800 for 10 licenses, however a proposal received from Axis 12 last year quoted £95 per license. Please can you explain why the cost has significantly risen and/or correct to the appropriate amount.

Response

The current cost of the licences is ~£106 ($149) per licence per month if paid upfront. The increase above £95 is due to changes in the exchange rate.

The cost provided by us includes the following:

- A buffer of to accommodate any further fluctuation in exchange rate (£50 across all licences)
- a charge for procuring them on CQC's behalf (@ ~£55 for 30 mins)
- a charge for implementing ten licenses (@ £975 for ~1.5 days' work to script, deploy and test additional licenses)

£55 + £975 + £50 (fluctuation) = £1080

£106 x 12 months x 10 licences = £12,720

Total: £13,800

CQ5 Managed Service: Configuration of New Relic licenses if CQC buys them. That option is missing. Please can you provide the option, alternatively provide a rationale as to why that option was not considered?

Response

If CQC bought them directly, the implementation cost would be £975 (subject to exchange rate fluctuations between now and the point of purchase)

CQ6 Commercial bid: The cost of licences from 3rd parties will most likely include VAT, which should be taken into account when adding 20% to the whole sum in the contract. Please can you confirm final costs with and without VAT for clarity?

Response

Managed service:

£192,780 ex VAT

£12,720 third-party licences

Total incl VAT: £244,056

Hosting (no third-party licences):

£190,260 ex VAT

£228,312 incl VAT

CQ7 Digital Hosting Commercial: 'Other' tab item 3 - the environment already exists so there shouldn't be a cost to building it? please clarify.

Response

The current public site development environment currently exists but is only available for use by Axis12 developers for development and code integration. This cost reflects the work required to move the environment to a new sector to make the development environment available for use by CQC and third-party developers.

CQ8 Digital Hosting Commercial: 'Other' tab item 6 - Please provide justification of the cost for the DR environment for the public website and the production environment, as these are the same specification but one is hosted on AWS, rather than in a Bunker datacentre. Therefore the cost should be less for the DR environment as in the case for the Provider Portal.

Response

The hosting prices have been offered at exactly the same cost as historic contracts. The OLS infrastructure, owing to its greater number of environments and servers, had a discount originally agreed, and this same discount has been offered as part of this contract.

CQ9 Digital Hosting Commercial: 'Other' tab item 8 - the environment already exists so there shouldn't be a cost to building it ? please clarify.

Response

The current Online Communities development environment currently exists but is only available for use by Axis12 developers for development and code integration. This cost reflects the work to move the environment to a new sector to make the development environment available for use by CQC and third-party developers.

CQ10 Digital Hosting Commercial: 'Other' tab item 15 ? Please can you explain why off-boarding costs have been included as part of this tender and not in previous tenders?

Response

We've included off-boarding costs of two days per platform to cover the cost of tasks associated with securely decommissioning the data and infrastructure at the termination of the contract. This wasn't explicit in previous contract but, to ensure transparency, it has been included in these costs.

CQ11 Digital hosting Commercial: 'Other' tab items 19-23 these look like a duplicate of items 3-6 in the support costs. See CQ2

Response

These are not duplicates. The tasks that have been requested require effort from both hosting supplier and managed service supplier and has been accounted for accordingly.

While the bulk of the work will be on the side of the hosting supplier, the managed service supplier will need to be involved in the configuration and testing once it's set up. We've allowed a little over an hour per system for this purpose.

CQ12 Commercial Bid: bidders were asked to apply a discount if successful in both Managed service and digital Hosting tender. For clarification purposes please can you calculate the total cost exc VAT if you were successful in both, taking into consideration the above clarification questions and responses.

Response

Total cost ex VAT: £307,360

(£203,500 (managed service) + £190,260 (hosting)) - (£24,000 (reduction for managed service) + £62,400 (reduction for hosting)

Schedule 11- Charges

		Total Cost: The Total cost for this Contract is: **£307,360 (ex VAT)** This is broken down as follows: - Hosting: £190,260 with a £62,400 reduction: Total: £127,860 - Managed Service £203,500 with a £24,000 reduction: Total:£179,500

The Detailed break-down of Charges is as follows:

Digital Hosting:

Total Costs:

	Financial years (April – March)					
	15/16	16/17	17/18	18/19	19/20	Total
	£	£	£	£	£	£
Staff costs	62400	0	0	0	0	62400
Consumables	0	0	0	0	0	0
Equipment	0	0	0	0	0	0
Travel expenses	0	0	0	0	0	0
Overheads	0	0	0	0	0	0
Sub contracts[1]	0	0	0	0	0	0
Other	127860	0	0	0	0	127860
Total costs	190260	0	0	0	0	190260
VAT (FINANCIAL year)	20%					0.2

If you are also bidding for CQC ICTC 554 - CQC Digital Hosting Managed Service please can you provide the discount to be applied should you be successful in both tenders.	
Discount to be applied	31.27 %

(£62,400 reduction - economies of scale would allow us to provide all support for both hosting and managed service in the 9 days allocated in the support contract)

Staff Costs:

Name	Role/Grade	Day Rates (£)	Staff time (days-15/16)
Various - see main document	PLANNED SYSTEM ADMINISTRATION 5.5 days per month.	650	66
Various - see main document	UNPLANNED SYSTEM SUPPORT Estimated liaison with support supplier 4 days per month for first three months	650	12
Various - see main document	AD HOC SYSTEM SUPPORT Estimated liaison with support supplier 2 days per month thereafter to roll over one month if unused	650	18

Other Expenses:

1	Other	Cost (£) Fy15/16
2	HOSTING Public site DEV environment	3720
3	BUILD Public site DEV environment	650
4	HOSTING Public site TEST environment	5580
5	HOSTING Public site PRODUCTION environment	14880
6	HOSTING Public site DR environment	14880
7	HOSTING Online communities DEV environment	3720
8	BUILD Online communities DEV environment	650
9	HOSTING Online communities PRODUCTION environment	11160
10	HOSTING Provider Portal DEV environment	8370
11	HOSTING Provider Portal TEST environment x 2	11160
12	HOSTING Provider Portal STAGE environment	14880
13	HOSTING Provider Portal PRODUCTION environment	18600
14	HOSTING Provider Portal DR environment	11160
15	OFFBOARDING Public site: 2 days Provider Portal: 2 days Online Communities: 2 days	3900
16	ONBOARDING	0
17	MIGRATION	0
18	PEN/SECURITY TESTING	0
19	CREATE Access to copy databases from Production to non-Production environments and vice versa: CQC public site	1300
2	CREATE Access to copy databases from Production to non-Production environments and vice versa: Provider	

Managed Service:

Total Costs:

	Financial years (April – March)					
	15/16	16/17	17/18	18/19	19/20	Total
	£	£	£	£	£	£
Staff costs	163800	0	0	0	0	163800
Consumables	0	0	0	0	0	0
Equipment	0	0	0	0	0	0
Travel expenses	0	0	0	0	0	0
Overheads	0	0	0	0	0	0
Sub contracts[1]	9000	0	0	0	0	9000
Other	30700	0	0	0	0	30700
Total costs	203500	0	0	0	0	203500
VAT (FINANCIAL year)	20%					0.2

If you are also bidding for CQC ICTC 558 - CQC Digital Hosting please can you provide the discount to be applied should you be successful in both tenders.		
Discount to be applied	£24,000.00	(Reduction of the cost of application penetration testing (£9,000), and system integration testing (£15,000), which will not be needed)

Staff Costs:

Name	Role/Grade	Day Rates (£)	Staff time (days/15/16)
Various (see main document)	PLANNED SUPPORT DAYS 9 days per month	650	108
Various (see main document)	AD HOC SUPPORT DAYS 12 days per month to roll over one month if unused	650	144

Sub-Contracts:

Organisation	Joint or sub- contractor	15/16
NCC	Subcontractor APPLICATION PENETRATION TESTING Provider Portal	3000
NCC	Subcontractor APPLICATION PENETRATION TESTING Public site	3000
NCC	Subcontractor APPLICATION PENETRATION TESTING Online Communities	3000

Other Expenses:

1	Other	Cost (£)-FY 15/16
2	SYSTEM INTEGRATION TESTING (estimated) Public site: 10 days Provider Portal: 10 days Online Communities: 4 days	15600
3	BUILD Access to all code repositories and branches	325
4	CONFIGURATION Ability to copy databases from Production to non-Production environments and vice versa	325
5	CONFIGURATION Ability to download databases and assets to create local dev environments	325
6	CONFIGURATION Ability to deploy code to all environments	325
7	NewRelic licences x 10: Provider Portal x 4 Public site x 4 Communities x 2	13800