

Framework Schedule 6A (Short Order Form Template and Call-Off Schedules)

Short Order Form

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Deliverables of Intangible Asset Valuation and dated 20 November 2025. It is issued under the Framework Contract with the reference number **RM6309**.

SECTION 1: CONTRACTING PARTIES

CALL-OFF REFERENCE:	CQC CPS 051
THE BUYER:	Care Quality Commission
BUYER ADDRESS	City Gate, Gallowgate, Newcastle, NE1 4PA
THE SUPPLIER:	PriceWaterHouseCoopers LLP (PwC LLP)
SUPPLIER ADDRESS:	1 Embankment Place London WC2N 6RH

SECTION 2: CALL-OFF CONTRACT TERM

CALL-OFF START DATE:	24 November 2025
CALL-OFF EXPIRY DATE:	23 February 2026
CALL-OFF INITIAL PERIOD:	3 Months
CALL-OFF OPTIONAL EXTENSION PERIOD	2 Months

SECTION 3: CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

Framework Ref: RM6309 Management Consultancy Framework Four (MCF4)
Project Version: v1.0
Model Version: v1.0

SECTION 4: CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

SECTION 5: PAYMENT METHOD

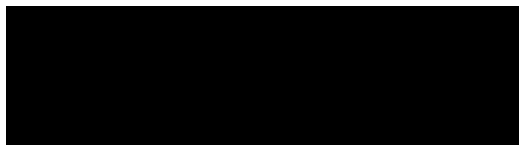
Payment in full following delivery of final report.

SECTION 6: BUYER AND SUPPLIER DETAILS

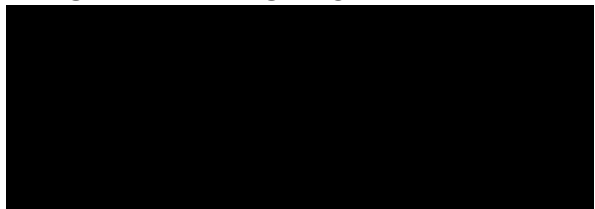
BUYER'S INVOICE ADDRESS:

accountspayable@cqc.org.uk

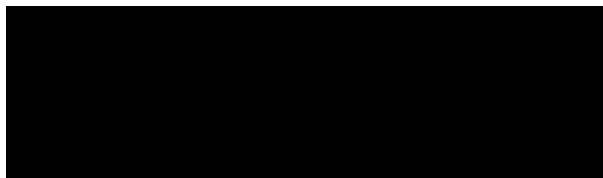
BUYER'S AUTHORISED REPRESENTATIVE



SUPPLIER'S AUTHORISED REPRESENTATIVE

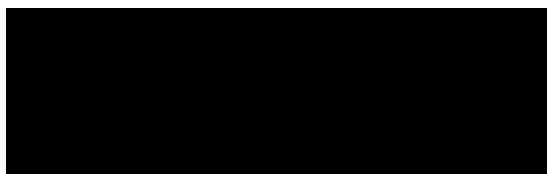


SUPPLIER'S CONTRACT MANAGER

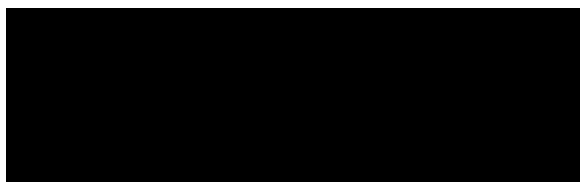


SECTION 7: KEY SUPPLIER STAFF

Key Staff (1):



Key Staff (2):



Key Staff (3):

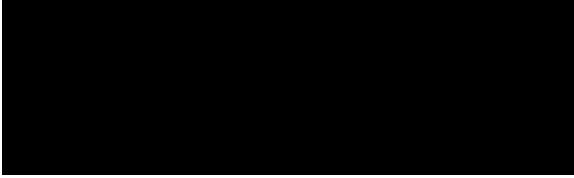
Framework Ref: RM6309 Management Consultancy Framework Four (MCF4)

Project Version: v1.0

Model Version: v2.0



Key Staff (4):



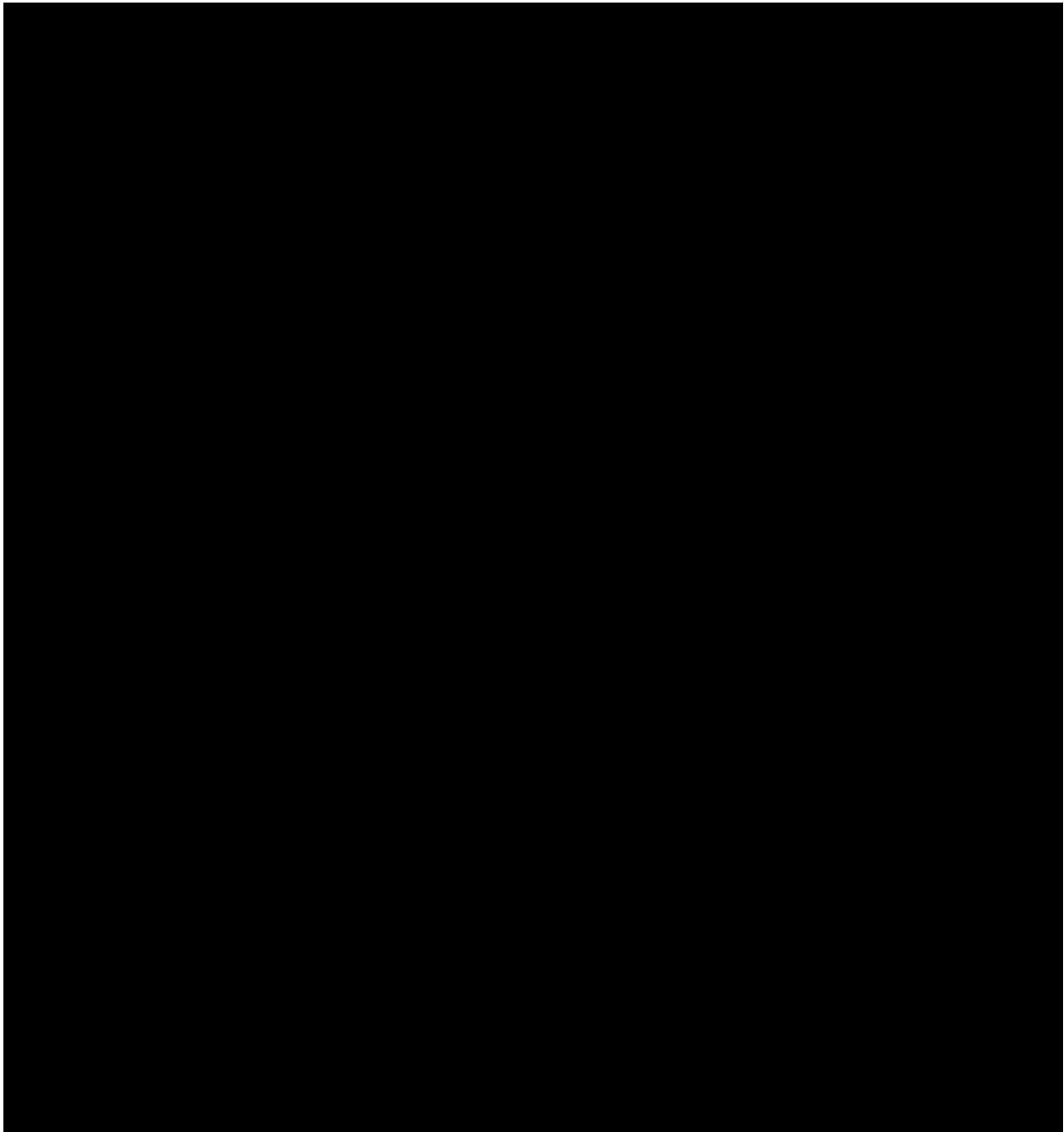
Key Staff (5):



SECTION 8: KEY SUBCONTRACTORS

N/A

SECTION 9: COMMERCIALLY SENSITIVE INFORMATION



SECTION 10: BUSINESS CONTINUITY DISASTER RECOVERY PLAN

SECTION 11: INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing, we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms
2. Joint Schedule 1 (Definitions)
3. Framework Special Terms
4. The following Schedules will be included in equal order of precedence:
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Call-Off Schedule 9 (Security)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility)
7. No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

SECTION 12: CALL-OFF SPECIAL TERMS

None

SECTION 13: MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

SECTION 15: REIMBURSABLE EXPENSES

None

Framework Ref: RM6309 Management Consultancy Framework Four (MCF4)

Project Version: v1.0

Model Version: v2.0

SECTION 16: SERVICE CREDITS

Not applicable

SECTION 17: PROCESSING DATA

The Buyer must confirm the following statements:

- That the Buyer has reviewed Joint Schedule 11 (Process Data) – Yes
- That Annex A has been completed by the Controller where applicable – Yes
- The roles for the processing of data under this Call-Off Contract will be:
Buyer - Controller
Supplier - Processor

SECTION 18: SECURITY

Part A: Short Form Security Requirements from Call Off Schedule 9 (Security) is applicable to this short Order Form.

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:

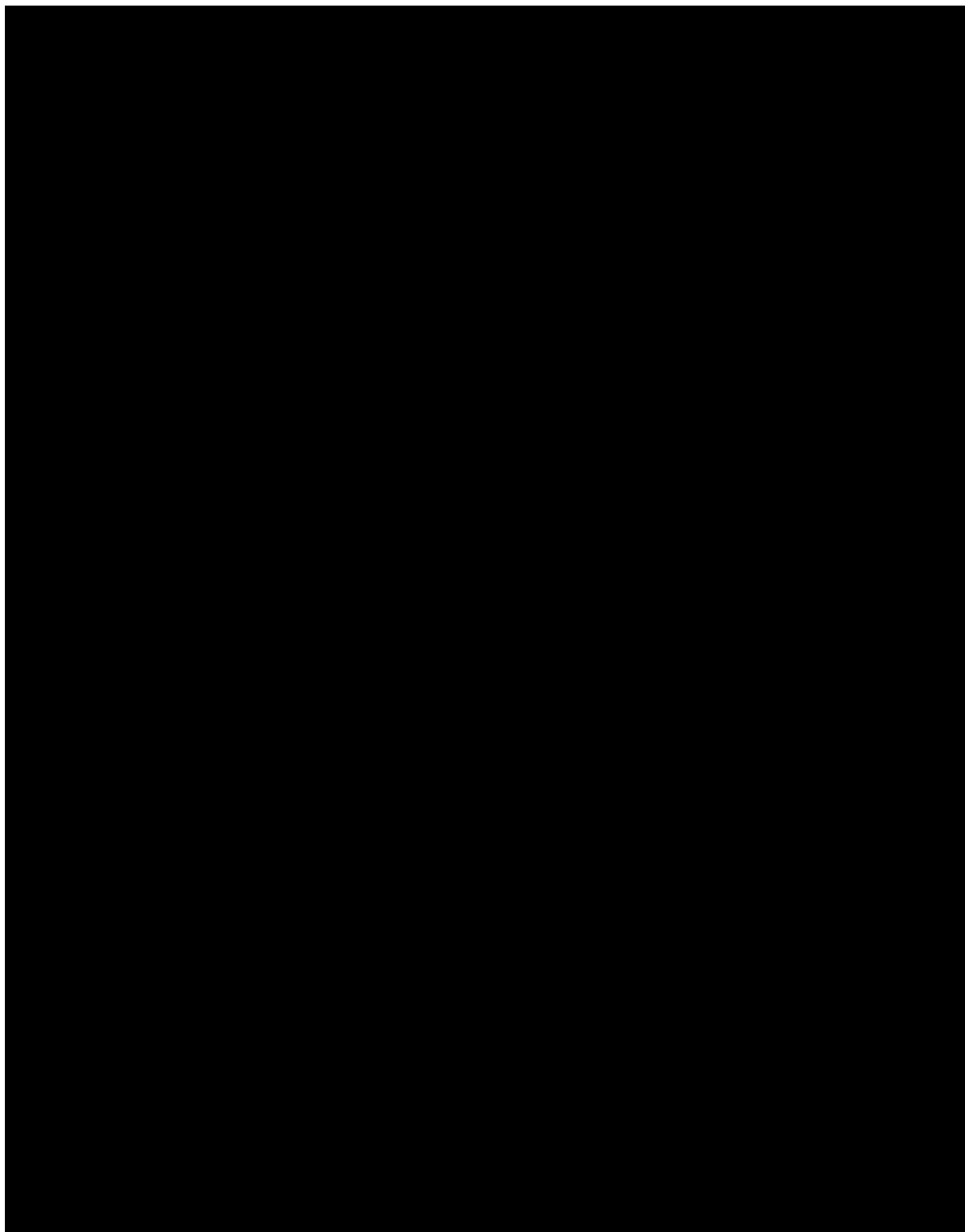
SIGNED for and on behalf of **PRICEWATERHOUSECOOPERS LLP**

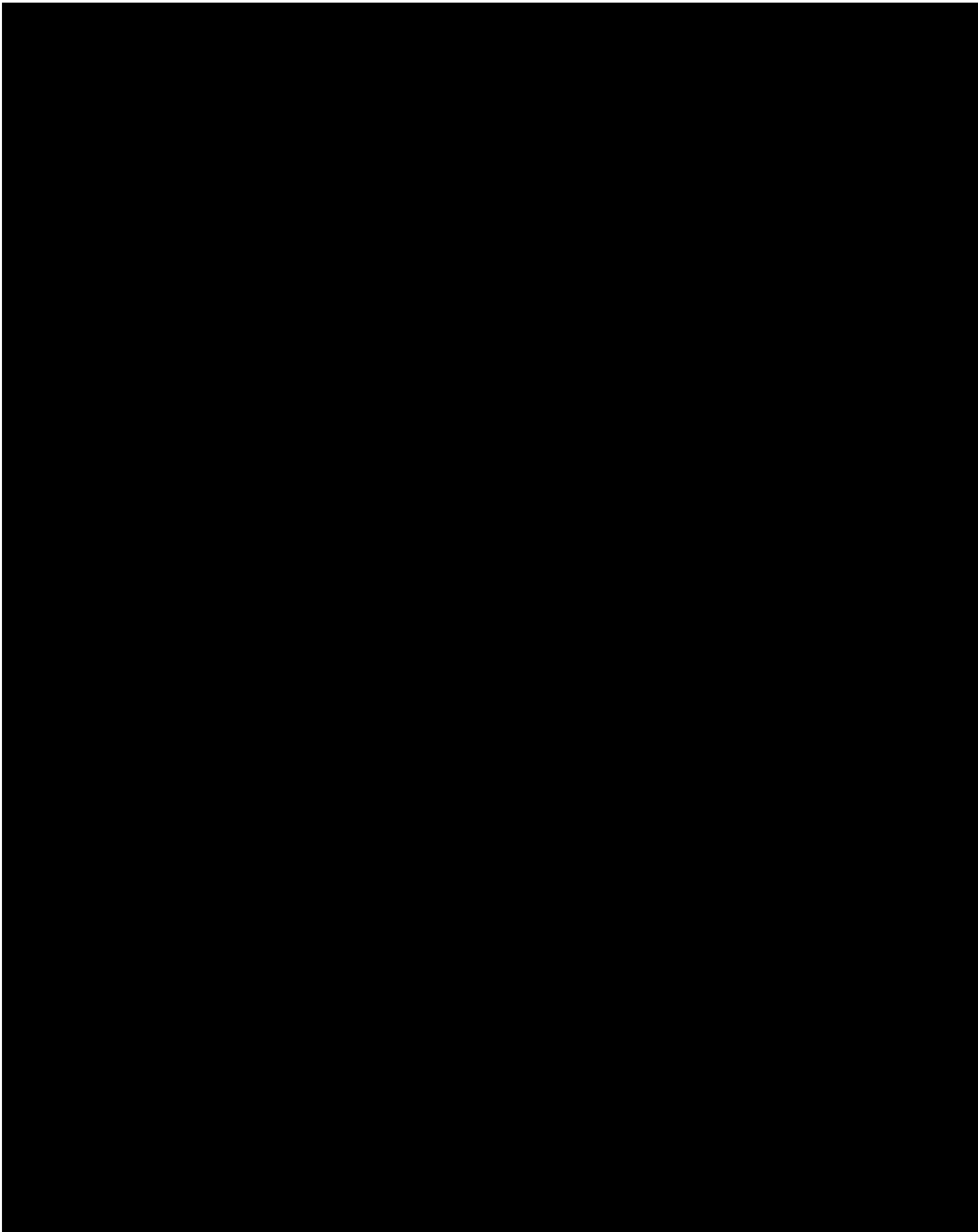
Authorised Signatory 1:

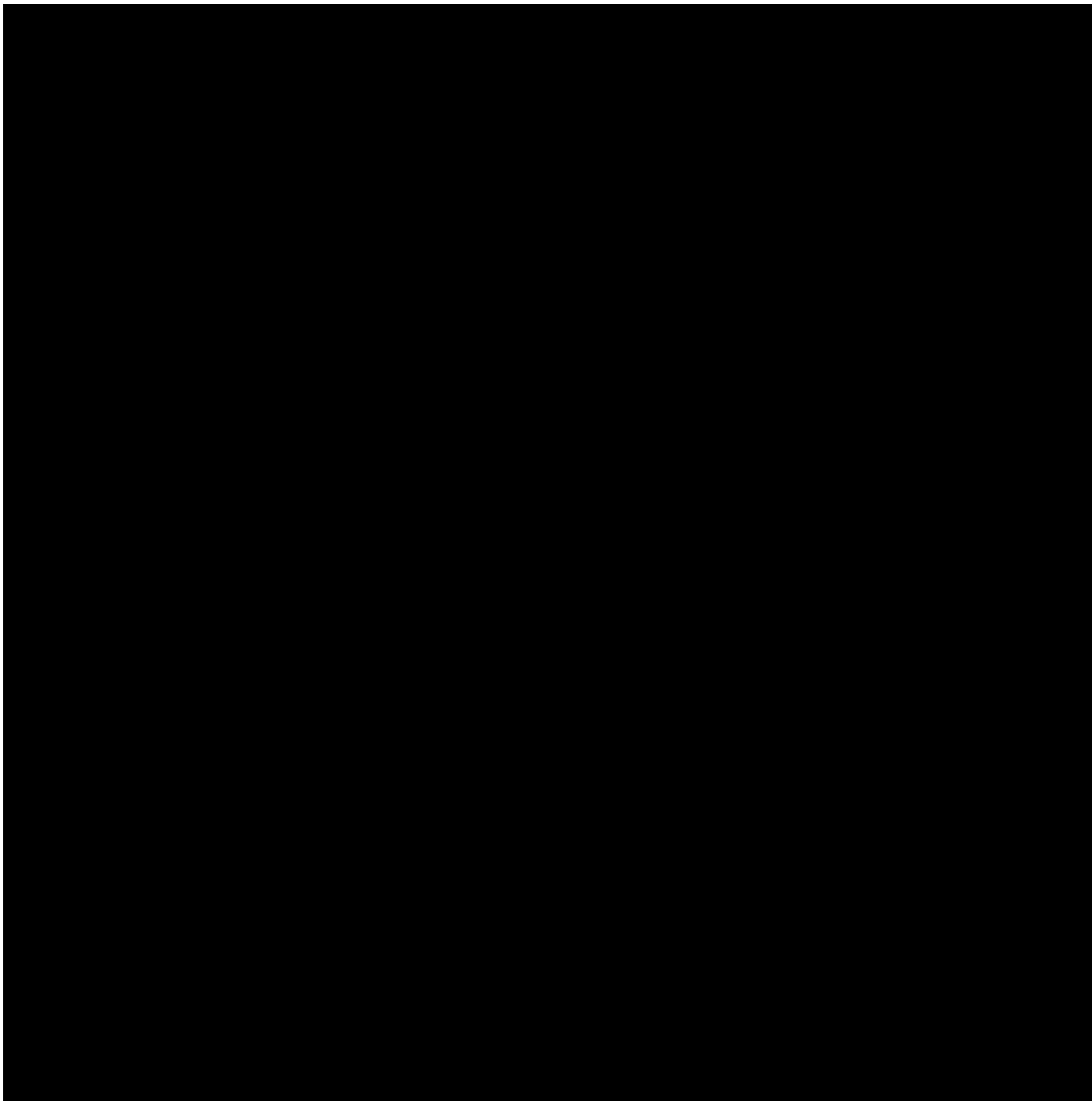
SIGNED for and on behalf of **PRICEWATERHOUSECOOPERS LLP**

Authorised Signatory 2:

Call-Off Schedule 4 (Call Off Tender)



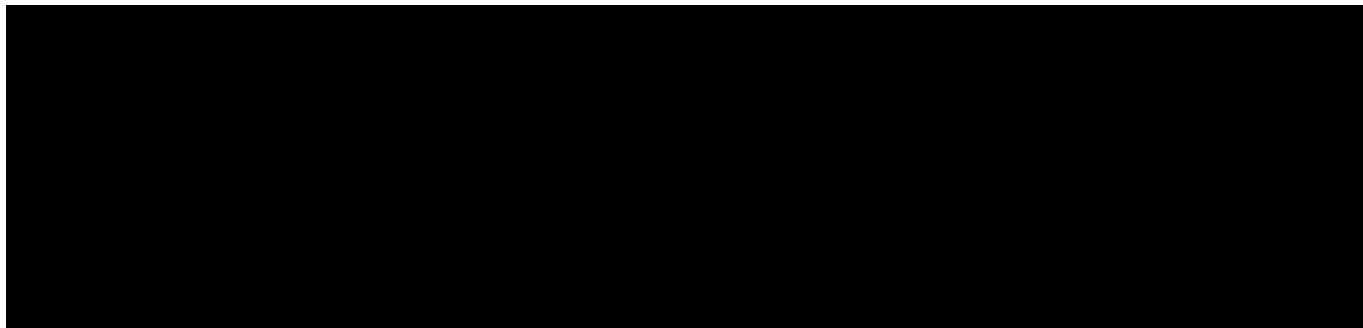




Call-Off Schedule 5 (Pricing Details)

The project will require the following budget:

Core scope: £95,000.00 Exc VAT (£114,000.00 Inc VAT)



Call-Off Schedule 20 (Call-Off Specification)

The Care Quality Commission (CQC) is the independent regulator of health and social care in England. The role of the CQC is to monitor, inspect and regulate services to make sure they meet fundamental standards of quality and safety, with the findings published to the public. See [Care Quality Commission](#) for more information.

CQC is an executive non-departmental public body whose statutory functions are set out in legislation. The sponsor department is the Department for Health and Social Care. CQC is accountable to Parliament through the Secretary of State for Health and the Chief Executive is the Accounting Officer.

CQC developed the Regulatory Platform (RP), a suite of applications, to modernise and support our regulatory approach. The transformation programme delivering RP concluded in March 2024 and resulted in the recognition of an intangible asset.

Subsequent events have indicated that RP is not delivering the intended value to CQC. This is in part due to RP not aligning to the way in which assessments are undertaken, but there are other deficiencies impacting upon performance which has led to CQC reverting to the legacy application, CRM, for registration processes and a hybrid approach has been introduced for assessment. These issues were highlighted in independent reviews by Dr Penelope Dash, Professor Sir Mike Richards and Peter Gill, which are referenced below.

An impairment review was carried out as part of our Annual Report and Accounts 2023/24, relying upon work undertaken by Peter Gill, however this did not provide sufficient detail or assessment of the service potential and consequently valuation of all applications that make up RP. This resulted in CQC being unable to provide sufficient assurance around the carrying value of the asset or the impairment charge included in the Financial Statements to the National Audit Office (NAO). This led to a qualification being placed on the audit opinion relating to the valuation of the regulatory platform intangible asset.

The preparation and audit of CQC's financial statements for 2024/25 requires us to complete an impairment review which will determine the appropriate value of the RP asset in our financial statements based on a formal technical valuation. It must also consider the timing of the impairment charge as to which financial year(s) it falls into.

Scope

CQC require (a) an assessment of the service potential and (b) a valuation of each of the 10 components of its Regulatory Platform (RP) for the purposes of impairment testing at the following dates 31 March 2023 and 31 March 2024.

The valuation will be subject to review by experts commissioned by NAO as part of their statutory audit of CQC's 2024/25 annual report and accounts. The supplier will be required to work alongside CQC to support the NAO review.

Basis of valuation

CQC's financial statements are prepared in accordance with the Financial Reporting Manual (FRM) issued by HM Treasury (HMT) as interpreted for the health sector in the Department of Health and Social Care Group Accounting Manual (GAM).

The GAM directs that as a non-cash generating intangible asset for which no active market exists RP should be valued at the cost of replacing its service potential.

CQC has had approval from HMT to adopt IAS38 for our 2024/25 financial year, in advance of the overall NHS deadline.

Timescales

We require this review and the output report to be completed by **19 December 2025**, as it will inform the opening intangible asset balance carried and any impairment charge for RP for the financial year 2024/25 in our draft financial statements to be presented to our Audit Committee in December. The output of the review will also be used by our external auditors as part of their work on our 2024/25 financial statements audit and the supplier is required to support any review undertaken by NAO on this topic.

References

- Dr Penelope Dash: [Review into the operational effectiveness of the Care Quality Commission](#)
- Professor Sir Mike Richards: [Review of CQC's single assessment framework and its implementation](#)
- Peter Gill: [Independent IT review](#)

Service Levels & Volumes

The supplier will be supported by the CQC Finance team.

It is expected that the supplier will outline the proposed programme to undertake the review based on their expertise and experience which will form the contractual service levels.

The outputs of this review must be completed by **19 December 2025**.

Authority Responsibilities

- Appoint a CQC representative within the Finance Team to act as the 'contract manager' who will be the main point of contact and oversee the work.
- CQC will ensure that the supplier has access to appropriate records/information and will facilitate all engagement with required CQC staff.

Contractor Responsibilities

- Appoint a point of contact to oversee the work and liaise with the CQC 'contract

manager' and other CQC staff as required.

- Produce a final report by 19 December 2025.
- Appoint a point of contact to support the review that NAO will conduct as part of their statutory audit of CQC's 2024/25 annual report and accounts.

Contract Management Arrangements

- The supplier will set out at the start of the contract a key delivery timeline including key milestones.
- Performance will be managed against achieving key targets in the project plan to the timeline agreed with CQC.
- It will be expected that at the start of the project, both CQC and the supplier organisation highlight key personnel who will be involved, their role and contact details.

Key Performance Indicators

Indicator	Measured by	Review Date
Delivery of a high-quality final report by required deadline	Production of the final report and sign off by CQC stakeholders	December 2025 / January 2026

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	[delete] as applicable: CCS / Buyer] ("CCS" "the Buyer") And [insert] name of Supplier] ("the Supplier")	
Contract name:	[insert] name of contract to be changed] ("the Contract")	
Contract reference number:	[insert] contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete] as applicable: CCS/Buyer/Supplier]	
Variation number:	[insert] variation number]	
Date variation is raised:	[insert] date]	
Proposed variation		
Reason for the variation:	[insert] reason]	
An Impact Assessment shall be provided within:	[insert] number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert] assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: 1. [CCS/Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ [insert] amount]
	Additional cost due to variation:	£ [insert] amount]
	New Contract value:	£ [insert] amount]

Framework Schedule 6A (Short Order Form Template and Call-Off Schedules)

Crown Copyright 2024

This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete]** as applicable: CCS / Buyer]

- Words and expressions in this Variation shall have the meanings given to them in the Contract.
- The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete]** as applicable: CCS / Buyer]

Signature	
Date	
Name (in Capitals)	
Address	

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature	
Date	
Name (in Capitals)	
Address	

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

- 1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:
 - 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
 - 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.
- 1.2 The Insurances shall be:
 - 1.2.1 maintained in accordance with Good Industry Practice;
 - 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
 - 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
 - 1.2.4 maintained for at least six (6) years after the End Date.
- 1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

- 2.1 Without limiting the other provisions of this Contract, the Supplier shall:
 - 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
 - 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
 - 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

- 4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

- 5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with

the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:
 - 1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);
 - 1.2 public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and
 - 1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[Guidance: Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[add] date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[add] cause]		
Anticipated impact assessment:	[add] impact]		
Actual effect of Default:	[add] effect]		
Steps to be taken to rectification:	Steps	Timescale	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[...]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	Steps	Timescale	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[...]	[date]	
Signed by the Supplier:		Date:	

Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[add] reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

“EU GDPR”	the General Data Protection Regulation ((EU) 2016/679);
“Joint Control”	where two or more Controllers jointly determine the purposes and means of Processing;
“Processor Personnel”	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller or further provided in writing by the Controller and may not be determined by the Processor.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) or as further provided in writing by the Controller, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, which are appropriate to protect against Personal Data Breach, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development;
 - (iv) cost of implementing any measures;and which shall be maintained in accordance with Data Protection Legislation and Good Industry Practice;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*)) and the Controller's further written instructions;
 - (ii) it uses all reasonable endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

- (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74 of the DPA 2018); or
 - (ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018, as well as any additional measures determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;
- (e) where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the transfer is in accordance with Article 45 of the EU GDPR; or

- (ii) the Processor has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the Controller which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under the EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations);
 - (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data; and
 - (f) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 7.** Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
- 8.** The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
- 9.** Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data

Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.
- 10.** The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 11.** The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 12.** The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 13.** Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
- (a) notify the Controller in writing of the intended Subprocessor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

- (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- 14.** The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
- 15.** The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
- 16.** The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office, any relevant Central Government Body and/or any other regulatory authority. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any non-mandatory guidance issued by the Information Commissioner's Office, relevant Central Government Body and/or any other regulatory authority.

Where the Parties are Joint Controllers of Personal Data

- 17.** In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

- 18.** With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
- 19.** Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
- 20.** Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
- 21.** The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:
- (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

- 26.** Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
- 27.** Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
- 28.** Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- 29.** Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

- 1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are:
[REDACTED]
- 1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **TO BE CONFIRMED**
- 1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">- During the course of the contract the Supplier will be provided access to key Authority documentation, financial data and staff.
Duration of the Processing	The processing shall be undertaken during the term of the contract only.
Nature and purposes of the Processing	The processing of data will be related to production of the final report presented to CQC.
Type of Personal Data	<p>During the course of the contract the Supplier may gather information relating to Authority employees such as names, job titles and their view around the scope of this project.</p> <p>Financial data may contain elements of personal data such as names, job roles, contact details. Details of suppliers and payments may also include the above mentioned personal data.</p>

Framework Ref: RM6309 Management Consultancy Framework Four (MCF4)

Project Version: v1.0

Model Version: v2.0

Categories of Data Subject	- Staff (including volunteers, agents, and temporary workers, suppliers)
International transfers and legal gateway	All data must be stored within the UK only.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All data must be destroyed by the Contractor at the end of the contract.

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

- 1.1** In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	<p>the occurrence of:</p> <ul style="list-style-type: none">a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/orb) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, <p>in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;</p>
"Security Management Plan"	<p>the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.</p>

2. Complying with security requirements and updates to them

- 2.1** The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 2.2** The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.3** Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.
- 2.4** If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request

by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

- 2.5** Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

- 3.1** The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.
- 3.2** The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:
- 3.2.1 is in accordance with the Law and this Contract;
 - 3.2.2 as a minimum demonstrates Good Industry Practice;
 - 3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and
 - 3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.
- 3.3** The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.
- 3.4** In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

- 4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

- 4.2.1 The Security Management Plan shall:
- a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;
 - b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;
 - c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables,

processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

- d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;
- e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;
- f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and
- g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

- 4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.
- 4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

- 4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.
- 4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

- 4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:
- a) emerging changes in Good Industry Practice;
 - b) any change or proposed change to the Deliverables and/or associated processes;
 - c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;
 - d) any new perceived or changed security threats; and
 - e) any reasonable change in requirements requested by the Buyer.
- 4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:
- a) suggested improvements to the effectiveness of the Security Management Plan;
 - b) updates to the risk assessments; and
 - c) suggested improvements in measuring the effectiveness of controls.
- 4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.
- 4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

- 5.1** Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- a) minimise the extent of actual or potential harm caused by any Breach of Security;
- b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;
- c) prevent an equivalent breach in the future exploiting the same cause failure; and
- d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.