

RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	FS900250
THE BUYER:	The Food Standards Agency
BUYER ADDRESS	Foss House, Kings Pool, 1-2 Peasholme Green, York, YO1 7PR
THE SUPPLIER:	Deloitte LLP
SUPPLIER ADDRESS:	1 New Street Square, London, EC4A 3HQ
REGISTRATION NUMBER:	OC303675
DUNS NUMBER:	364807771
SID4GOV ID:	N/A

Applicable framework contract

This Order Form is for the provision of the Call-Off Deliverables and dated 30th September 2022.

It's issued under the Framework Contract with the reference number RM6187 for the provision of **FS900250 Strategic Partner to Support Delivery programmes**.

CALL-OFF LOT(S):
Lot 2: Strategy & Policy

Call-off incorporated terms

The following documents are incorporated into this Call-Off Contract.

Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.

2. Joint Schedule 1 (Definitions and Interpretation) RM6187
3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 9 (Minimum Standards of Reliability)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility) - Mandatory
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

Supplier terms are not 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.

Call-off special terms

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1 - The Buyer is only liable to reimburse the Supplier for any expense or any disbursement which is

- (i) specified in this Contract or*
- (ii) which the Buyer has Approved prior to the Supplier incurring that expense or that disbursement. The Supplier may not invoice the Buyer for any other expenses or any other disbursements*

Special Term 2 - Supplier's tender is true and accurate to the best of its knowledge and is based on the accuracy of the information supplied by the Buyer and/or on its behalf.

Special Term 3 - The Parties may from time to time agree statements of work containing details of the specific Services and Deliverables contracted for by Buyer on the terms of the agreed Call-Off Contract.

Special Term 4 - Any project timelines are indicative and intended solely for planning purposes, and will depend on all parties fulfilling their responsibilities, including timely provision of accurate information.

Special Term 5 - If the scope of Services, assumptions, dependencies, content of the ITT, and/or Buyer responsibilities prove to be inaccurate, the Parties will address this as a Variation.

Special Term 6 - Supplier may terminate the Call-Off Contract upon written notice to Buyer if the performance of any part of the Services would conflict with law, professional rules or Supplier's independence. Supplier agrees to provide as much notice to Buyer as is reasonably possible and will work with Buyer to seek to mitigate any impact on the Services and/or the project.

Special Term 7 - Supplier Existing IPR includes any enhancements and/or modifications developed in the course of providing the Services.

Special Term 8 - The Deliverables are for Buyer's exclusive use and provided for the purposes described in this Call-Off Contract. No person other than Buyer may rely on the Deliverables and/or information derived from them. This does not affect the Buyer's right to sub-licence any New IPR or Specially Written Software that may be supplied under the Call-Off Contract.

Special Term 9 - The Buyer will either provide written confirmation that Deliverables and Milestones are accepted, or provide reasons for their non-acceptance, within 10 Working Days of their receipt or completion (whichever is earlier), except where explicitly agreed in the scope of work. If the Buyer does not do this, the relevant Deliverable and/or Milestone will be deemed to be finally accepted. Any subsequent repair or replacement warranty period will only apply if agreed as a Variation.

Special Term 10 - Supplier shall not update, upgrade, maintain or provide new versions of any Deliverable after the date on which the final Deliverable is accepted.

Special Term 11 - Supplier will store and back up government data according to its own data storage policies.

Special Term 12 - Where Supplier is required to use the software, products or services of Buyer's third-party vendor, the Buyer shall ensure that it has the rights to allow the Supplier to use such software, products or services and that they shall meet the Buyer's requirements.

Special Term 13 - Supplier Staff will be entitled to any absence(s) as agreed between the Parties.

Special Term 14 - Buyer will not require any Supplier Staff to enter into any direct confidentiality agreement(s).

Special Term 15 - The Supplier is not an intermediary to which any of the conditions in s61N Income Tax (Earnings and Pensions) Act 2003 apply. The Supplier may use equity partners, who are self-employed for tax, in the delivery of the Services, but must inform the FSA if this is the case.

Special Term 16 - Buyer will supply Supplier with any internal policies, codes, standards or procedures that Buyer requires Supplier complies with, prior to the start of the Services. Supplier must only comply with such policies, codes, standards or procedures if they do not increase the costs of the Supplier; increase the scope of the Services; or conflict with any policy or regulatory obligation of the Supplier.

Special Term 17 – In order for Supplier to complete its work to the required standard within anticipated timescales, Supplier assumes that Buyer will provide Supplier on a timely basis with (i) instructions and access to Buyer personnel and (if applicable) premises, and (ii) accurate and complete information. Supplier will also assume that Buyer will inform Supplier promptly if Buyer's requirements change.

Special Term 18 – Whilst Supplier may review and comment on legal agreements, Supplier is not qualified to provide legal advice. Accordingly, where Supplier reviews sections of draft agreements prepared by Buyer or its legal advisers, or provide a formula, calculation, table or otherwise for inclusion in a legal agreement, or both, it is the responsibility of Buyer's legal advisers or Buyer (as applicable), to ensure that the drafting of that document effectively reflects the commercial agreement that the parties to it have reached. Where Supplier engages Deloitte Legal services as part of its delivery, this is to provide subject matter expertise only and will not constitute legal advice.

Special Term 19 – Buyer has not stated a requirement for a model in the specification. Should this requirement arise in future work packages, Supplier will discuss and agree the model's specification with Buyer and set out its agreed proposed content, form and functionality in a specification document. Supplier will send Buyer updates and drafts of the model during its development and populate it with the data Buyer requires. Supplier will draft user instructions including key assumptions that have been agreed with Buyer. Drafts and user instructions should be destroyed once they are superseded by the final version of the model, in order to avoid any confusion over version control.

Special Term 20 – Supplier will subject the model to development testing before the final draft version is sent to Buyer for Buyer's own acceptance testing, and Supplier recommends that Buyer carries out its own testing on it, so Buyer can verify that it meets its requirements. Under the model release process Buyer will acknowledge that it has completed its acceptance testing and accepts responsibility for the model, including its assumptions, input data, outputs and associated documentation. Given the nature of a model, it is not generally possible to test it to verify that it is error-free.

Special Term 21 – During the Services, if Supplier gives Buyer draft Deliverables or oral advice, this will be on the understanding that Buyer will only rely on the final Deliverables, as any draft Deliverables or oral advice are necessarily work in progress and subject to change before they are confirmed in a final Deliverable.

Special Term 22 – During the Services, Supplier will not audit, test or verify any information given to it, unless the scope of Services includes such an exercise. Further, if Supplier gives you spreadsheets or models to illustrate its advice, these will not be Deliverables unless they are listed as such in the Call-Off Contract (and/or specific work packages), so they will therefore be given to Buyer solely on a non-reliance basis.

Special Term 23 – We will agree the scope, requirements and approach to any data handing and/or processing requests with you on an individual work packages basis.

Call-off start date: 3rd October 2022

Call-off expiry date: 2nd October 2024

Call-off initial period: 2 years

Call-off deliverables:

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

Security

Short Form security requirements apply

and

Security Policy, to be shared within 3 months of Contract award (and subject to review and agreement of Supplier).

Maximum liability

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

The Estimated Year 1 Charges used to calculate liability in the first contract year are:

£1.5 million Estimated Year 1 Charges of the Contract.

Call-off charges

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

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law

Reimbursable expenses

Recoverable as stated in Framework Schedule 3 (Framework Prices) paragraph 4.

Payment method

Payment will be made by BACS monthly in arrears. Payment terms will be included in each statement of work should they differ.

Buyer's invoice address

SSCL

[REDACTED]

Food Standards Agency

PO Box 796

Newport

NP10 8FZ

The supplier will provide invoices with a valid purchase order number to SSCL at [REDACTED]
[REDACTED] for processing with a copy sent to
[REDACTED]

FINANCIAL TRANSPARENCY OBJECTIVES

The Financial Transparency Objectives do not apply to this Call-Off Contract.

Buyer's authorised representative

[REDACTED]

[REDACTED]

Foss House,

Kings Pool,

Peasholme Green,

York,

YO1 7PR

Supplier's authorised representative

[REDACTED]

[REDACTED]

[REDACTED]

Deloitte

1 New Street Square,


London,

EC4A 3HQ

Supplier's contract manager

[REDACTED]

[REDACTED]


Deloitte
1 New Street Square,
London,
EC4A 3HQ

Progress report frequency

Quarterly meetings to be held with the supplier for the overarching call-off Contract, although we may look to increase or decrease this over the lifetime of the Contract. Weekly reports provided at progress meetings expected for Work Package 1.

Progress meeting frequency

Quarterly meetings to be held with the supplier for the overarching call-off Contract, although we may look to increase or decrease this over the lifetime of the Contract. Weekly reports provided at progress meetings expected for Work Package 1.

Key staff

See Call Off Schedule 7

Key subcontractor(s)

Any key subcontractors for future work will be included in the individual statement of works.

Commercially sensitive information

See Joint Schedule 4

Service credits

Not applicable

Additional insurances

Not applicable

Guarantee

Not applicable

Buyer's environmental and social value policy



FSA Environmental
Sustainability Strate

Social value commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

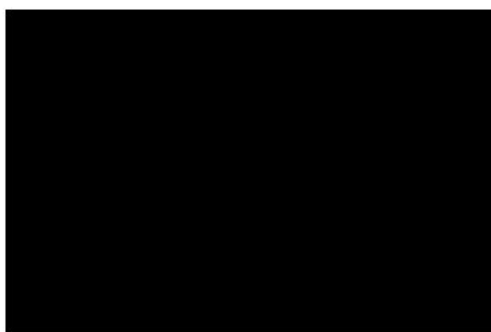
The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Supplier:

Signature:



For and on behalf of the Buyer:



Joint Schedule 4 (Commercially Sensitive Information)

What is Commercially Sensitive Information?

- i. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- ii. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- iii. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	30/09/2022	Any information relating to: personal information (CVs, contact details, etc.)	6 years
2	30/09/2022	Any information relating to: pricing and details of Supplier's cost base	6 years
3	30/09/2022	Any information relating to: insurance arrangements	6 years
4	30/09/2022	Any information relating to: proprietary information	6 years
5	30/09/2022	Any information relating to: approach and/or methodologies	6 years

Joint Schedule 6 (Key Subcontractors)

Restrictions on certain subcontractors

- iv. The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- v. The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
- vi. Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - i. the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - ii. the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - iii. the proposed Key Subcontractor employs unfit persons.
- vii. The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - i. the proposed Key Subcontractor's name, registered office and company registration number;
 - ii. the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - iii. where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;
 - iv. for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - v. for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
 - vi. (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

- viii. If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
 - i. a copy of the proposed Key Sub-Contract; and
 - ii. any further information reasonably requested by CCS and/or the Buyer.
- ix. The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
 - i. provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - ii. a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - iii. a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - iv. a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - v. obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
 - 1. the data protection requirements set out in Clause 14 (Data protection);
 - 2. the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - 3. the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;
 - 4. the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - 5. the conduct of audits set out in Clause 6 (Record keeping and reporting);
 - vi. provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - vii. a provision restricting the ability of the Key Subcontractor to subcontract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 11 (Processing Data)

Definitions

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

“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

- xi. 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:
- i. “Controller” in respect of the other Party who is “Processor”;
 - ii. “Processor” in respect of the other Party who is “Controller”;
 - iii. “Joint Controller” with the other Party;
 - iv. “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

- xii. 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.
- xiii. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
- xiv. 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:
 - i. a systematic description of the envisaged Processing and the purpose of the Processing;
 - ii. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

- iii. an assessment of the risks to the rights and freedoms of Data Subjects; and
- iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- xv. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
 - i. Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - ii. ensure that it has in place Protective Measures, 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 (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - 1. nature of the data to be protected;
 - 2. harm that might result from a Personal Data Breach;
 - 3. state of technological development; and
 - 4. cost of implementing any measures;
 - iii. ensure that :
 - 1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - 2. it takes all reasonable steps 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;
 - iv. 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:
 - 1. the Controller or the Processor has provided appropriate

- safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
 - 2. the Data Subject has enforceable rights and effective legal remedies;
 - 3. the Processor complies with its obligations under the 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
 - 4. 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
- v. 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.
- xvi. 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:
 - i. receives a Data Subject Access Request (or purported Data Subject Access Request);
 - ii. receives a request to rectify, block or erase any Personal Data;
 - iii. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - iv. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - v. 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
 - vi. becomes aware of a Personal Data Breach.
- xvii. 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.
- xviii. Taking into account the nature of the Processing, the Processor shall provide the Controller with 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 by immediately providing:
 - i. the Controller with full details and copies of the complaint, communication or request;

- ii. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - iii. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - iv. assistance as requested by the Controller following any Personal Data Breach; and/or
 - v. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- xix. 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:
- i. the Controller determines that the Processing is not occasional;
 - ii. 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
 - iii. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- xx. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- xxi. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- xxii. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
- i. notify the Controller in writing of the intended Subprocessor and Processing;
 - ii. obtain the written consent of the Controller;
 - iii. 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
 - iv. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
- xxiii. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
- xxiv. 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).

- xxv. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. 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 guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

- xxvi. 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

- xxvii. 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.
- xxviii. 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.
- xxix. 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.
- xxx. 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.
- xxxi. The Parties shall only provide Personal Data to each other:
- i. to the extent necessary to perform their respective obligations under the Contract;
 - ii. 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
 - iii. where it has recorded it in Annex 1 (*Processing Personal Data*).
- xxxii. 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.

- xxxiii. 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.
- xxxiv. 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”**):
 - i. 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
 - ii. 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:
 - 1. 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
 - 2. 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.
- xxxv. 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:
 - i. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - ii. implement any measures necessary to restore the security of any compromised Personal Data;
 - iii. 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
 - iv. 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.
- xxxvi. 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).

- xxxvii. 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)*.
- xxxviii. 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: [REDACTED]

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 for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor 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: This schedule will be completed for each individual work package.
Duration of the Processing	3 rd October 2022 - 2 nd October 2024
Nature and purposes of the Processing	This schedule will be completed for each individual work package.
Type of Personal Data	This schedule will be completed for each individual work package.

Categories of Data Subject	This schedule will be completed for each individual work package.
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	This schedule will be completed for each individual work package.

Call-Off Schedule 5 (Pricing Details)

COST OR VOLUME DISCOUNTS - INNOVATION

The Food Standards Agency collaborates with our suppliers to improve efficiency and performance to save the taxpayer money.

A tenderer should include in his tender the extent of any discounts or rebates offered against their normal day rates or other costs during each year of the contract. Please provide full details below:

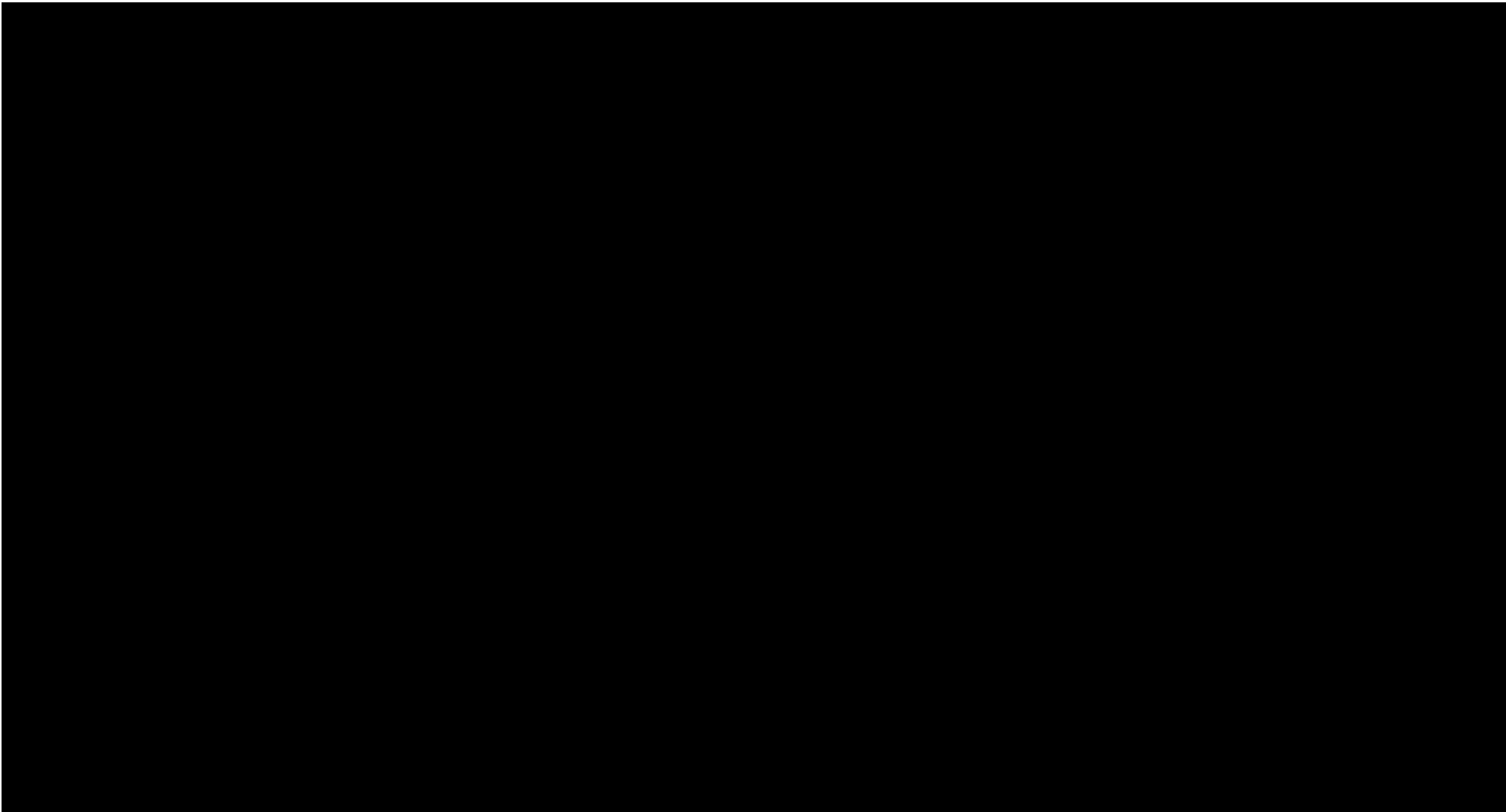
Deloitte response:

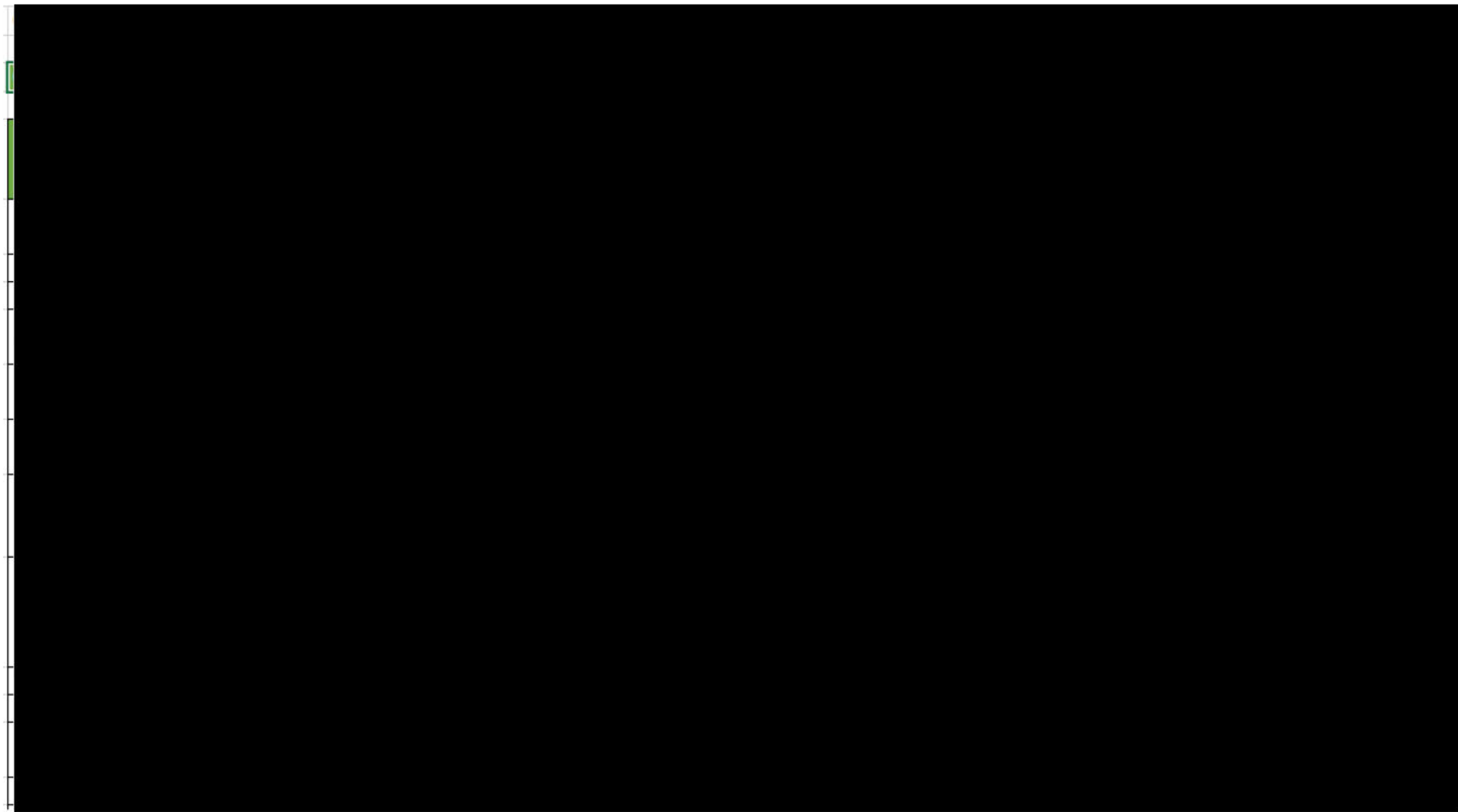
[Redacted response content]

[illegible]

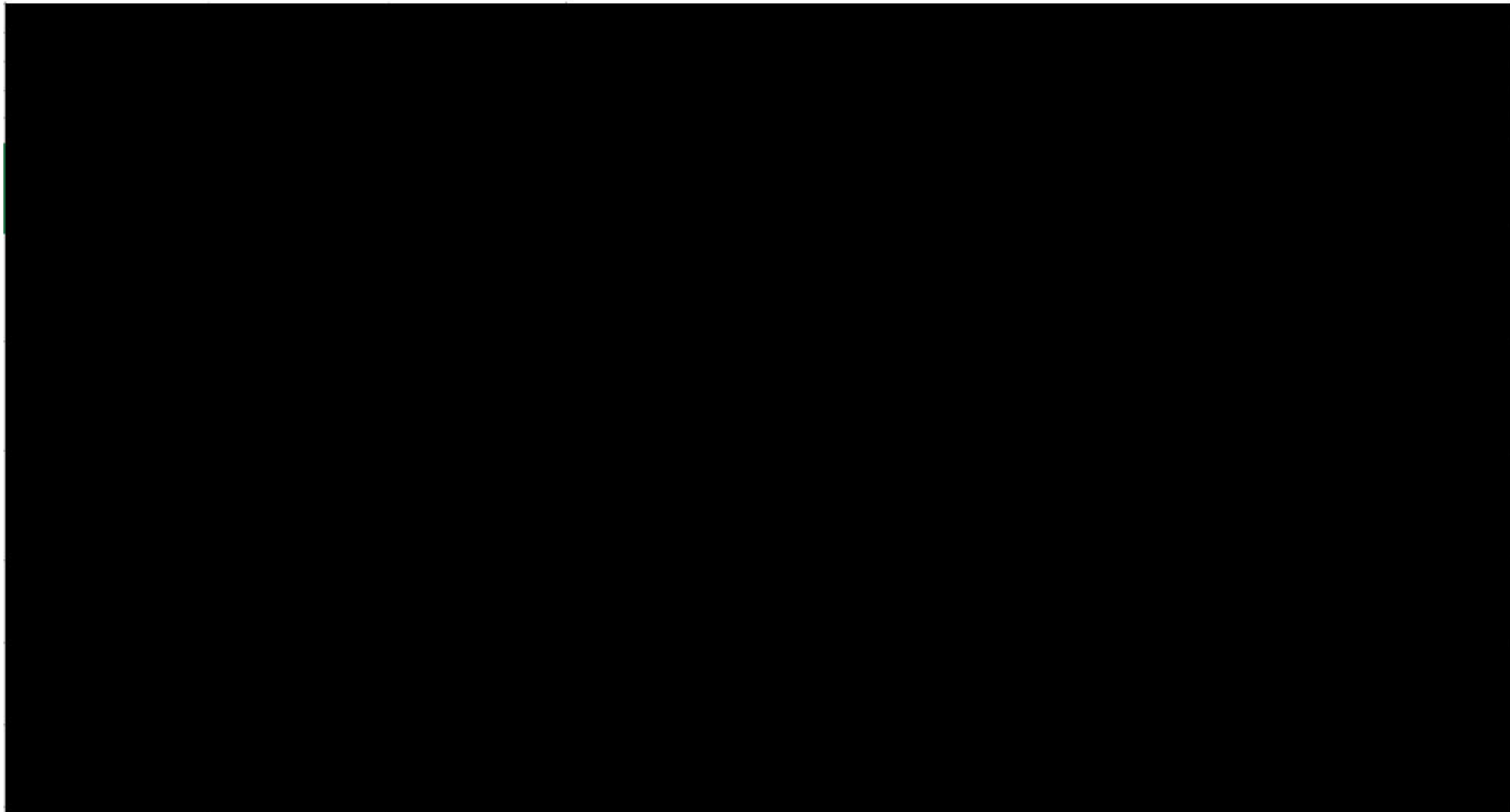
		Total Cost:	£97,500.00
		<i>Discount applied to Work Package 1:</i>	
		<i>Discounted average daily rate for Work Package 1:</i>	

Comments/Notes:
Deloitte response





The table content is completely redacted by a large black rectangle. Only the leftmost column, which appears to be a list of rows, is visible as a narrow strip on the left edge of the redacted area.



Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Order Form lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
 - 1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
 - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - 1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;
 - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
 - 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.
- 1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff

Annex 1- Key Roles

Key Role	Key Staff	Contact Details
Lead FSA Partner		
Lead Commercial Advisory Partner		
Strategic Partnership Director		

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>1 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>2 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>3 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 has been 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.

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Specification Reference
<i>FS900250</i>
Specification Title
<i>Strategic Partner to Support Delivery programmes</i>
Contract Duration
<i>12th September 2022 – 11th September 2024 (optional 12-month extension)</i>

This specification, which forms part of the Invitation to Tender (ITT), comprises of three individual sections: -

- A. SPECIFICATION:** An outline of the requirement
- B. PROCUREMENT TIMETABLE:** An estimated timetable for the procurement of the proposed requirement
- C. TENDER REQUIREMENTS AND EVALUATION CRITERIA:** Provides guidance to applicants on the information that should be included within tenders and on the evaluation criteria and weightings used by evaluators when assessing and scoring tenders

Tenders for FSA funded projects must be submitted through the FSA E-sourcing and contract management system, ECMS, using the following link: <https://food.bravosolution.co.uk/web/login.html>. Failure to do so may result in the tender response not being processed by the system or the response being automatically disqualified during the evaluation stage of the tender process.

THE SPECIFICATION, INCLUDING PROJECT TIMETABLE AND EVALUATION OF TENDERS

GENERAL INTRODUCTION

The Food Standards Agency is an independent Government department working across England, Wales and Northern Ireland to protect public health and consumers wider interest in food. We make sure food is safe and what it says it is.

- The Agency is committed to openness, transparency and equality of treatment to all suppliers. As well as these principles, for science projects the final project report will be published on the Food Standards Agency website (www.food.gov.uk). For science projects we will encourage contractors to publish their work in peer reviewed scientific publications wherever possible. Also, in line with the Government's Transparency Agenda which aims to encourage more open access to data held by government, the Agency is developing a policy on the release of underpinning data from all of its science- and evidence-gathering projects. Data should be made freely available in an accessible format, as fully and as promptly as possible. Consideration should be given to data management as new contracts are being negotiated. Resource implications for this should be taken into account. The mechanism for publishing underpinning data should allow the widest opportunity for to enable its re-use. Where possible, underpinning data should be included in the final project report. Where data are included in the final report in pdf format, they should also be published separately in a format that can be used for further analysis. Large data sets can be provided separately in an annex to the report, and published, where possible, alongside the final report online. Where it is more appropriate to publish underpinning data in an existing database, archive, repository or other community resource, or for data to be saved in a specialist proprietary format, information will be provided on how the data can be accessed. There will be some circumstances where release of data may need to be restricted or anonymised for reasons of commercial and/or personal sensitivities.

The FSA undertakes Official Controls (OCSs) as set out in EU regulations to ensure food is safe to eat, food is what it says it is and animal welfare is protected on behalf of Defra (the policy lead).

Transformation within FSA is currently being progressed via several large scale delivery projects and/or programmes as follows: -

Operational Delivery

Operational Delivery consists of a number of teams, support will be primarily required across The Field Operations Division and The Operational Assurance and Transformation Division (OAT)

The Field Operations Division is spread across three geographical regions within England and Wales – North, East and Wales & West and the central Change Business Implementation (CBI) unit. Our field staff teams consist of Operations Managers, Veterinary Field Leaders, Veterinary Field Coordinators, Area Managers, Inspection Team Leaders and Meat Hygiene Inspectors along with support and project team members.

Field Operations is responsible for:

- Delivery of official controls in FSA approved meat establishments in England and Wales, including official controls for meat.
- Milk production hygiene inspections in England and Wales.
- Enforcement of EU wine regulations through inspections of premises and traders across the UK.
- Facilitating third country exports, carrying out on-site assessment visits relating to the recommendation of approval for premises in England and Wales and auditing the approved premises against the third country requirements.
- Within Field Operations, CBI is responsible for:
 - Meeting business priorities and acting as the strategic gate keeper to Field Operations.
 - Effectively landing change in the division and working together with a range of stakeholders to maintain and challenge business delivery.

OAT undertakes a wide array of activities for the Agency and is responsible for providing the second line of assurance as an oversight role separate from those responsible for operational delivery and specific functions within the Operations Group directorate. It also seeks to modernise how the FSA delivers official controls as a regulator.

Areas of work identified as requiring support, with an expected start date of September are: -

- The Review of Operational Functions – to review and/or redesign operational functions with a focus on the effectiveness of the performance framework, assurance delivered and change management capability.
- The Target Operating Model – the design of a Target Operating Model in Operations based on planned strategic changes to resourcing.

A full specification will be provided as each work package is commissioned.

Specialist support may also be required to support the retender of the six geographical contracts for Delivery of Official Controls Contracts for England and Wales, the retender workstream is due to commence in Autumn 2022

Operational Transformation Programme (OTP)

OTP sits within OAT and is a complex programme of change, seeking to modernise the delivery of Official Controls in the meat, dairy and wine industries (initially focusing on the meat sector). Full-scale transformational change will require a shift in both legislation and culture and will consequently take several years to complete, but a number of short/medium-term opportunities to deliver meaningful change are being pursued in the interim. Central to the Programme is the Future Delivery Model (FDM) which sets out our aspirations to introduce a more risk-based and proportionate approach to regulation in the meat industry area rather than the current 'one size fits all' system. OTP builds on earlier initiatives, including the meat strand of the Regulating our Future (RoF) Programme, the joint FSA/Food Standards Scotland (FSS) Cutting Plant & Cold Store review of 2018, and the more recent and more broadly based analysis within the Strategic Review of Official Controls (SROC) which was concluded in April 2019.

Whilst the current model is not broken and continues to ensure the required food hygiene and animal welfare controls are comprehensively delivered, there are some aspects that could be improved in a reformed Operating Model:

- **Accountability** – recasting the balance of accountability between industry and the FSA by increasing the responsibility of food business operators (FBOs) in the production of safe food and moving to a more risk-based and proportionate approach to regulation and resource deployment being underpinned by a set of rules, standards &

guidance for compliance. This will demonstrate that, as the regulator, we expect compliance by default, and develop a clear set of sanctions and incentives to be applied to those who fail to comply.

- **Value for Money** – developing a more robust, efficient and sustainable Operating Model that optimises delivery of our Regulatory Assurance function?
- **Technology** – higher processing speeds and increased automation in food production, presents both opportunities and challenges and requires the introduction of technological solutions that remove waste, reduce variation and improve compliance with food standards to improve compliance and reduce public health risk.
- **Responsiveness** – Consumer needs are becoming more sophisticated and fragmented. We need to develop improved working practices with industry to ensure the FSA is aware of changes in national and international food production and can plan for these. The Operating Model needs to be sufficiently agile to respond to emerging needs and to food-based incidents.
- **Trust and Food Safety** – Consumer confidence in food safety needs to be maintained and improved. We should seek to develop new assurance protocols, exploring the opportunities for data sharing and publication of compliance data to generate increased trust in the industry, which could also benefit future export trade.
- **Trade** – Our exit from the EU could change the balance of production between the export and domestic markets, as well as the regulations we are governed by (Official Control Regulations, 625/2017). We need to develop an Operating Model that maximises opportunities available to us through 627/2017 and to support international trade.
- **Resource Availability** – any concerns about the future supply of OV and OA resource could be mitigated by developing an Operating Model which is less resource intensive and changes the current demand.

FSADOC Contingency Planning

FSA are the central competent authority for the delivery of official controls in FSA approved establishments in England and Wales. These official controls are delivered through 6 geographical contracts by a single supplier.

Following the collapse of Carillion in 2018, which affected 450 public sector contracts, there is increased scrutiny across government contracts. Part of that scrutiny is around the development of contingency plans for supplier failure, particularly for single supplier delivery models.

FSA require a strategic delivery partner to support FSA in the preparation and implementation of a skeleton GovCo to allow the GovCo to step in should the supplier fail and maintain the delivery of the services.

Project to commence 12th September 2022 and be completed by 31st January 2023.

Achieving Business Compliance (ABC)

The food regulatory system plays a critical role in protecting the public, and the UK economy, from the risks of costly and damaging foodborne disease outbreaks or food scandals and maintaining the high reputation of the UK food industry. But the food sector has changed dramatically in the three decades since the current regulatory system was introduced. Although regulation has continued to evolve, our assurance model has not kept pace with the significant changes in the food industry. The Food Standards Agency is committed to ensuring that food remains safe, and consumers continue to have food they can trust in the future. So, in a rapidly evolving food landscape we need to regulate in a smarter way to make sure that food is safe and what it says it is.

The FSA has established the ABC programme, through which we will develop a set of smarter regulatory approaches, which: make it easier for businesses to provide safe and trusted food for consumers; target regulatory resources at the areas which pose the greatest risk; and improve

compliance across the system by working with and through others, including regulatory partners and influential businesses – a key enabler to delivering against the FSA Strategy 2022 - 2027

The programme is organised into three key strands of work:

1. Making regulation more targeted and proportionate for all the food businesses regulated by local authorities.
2. Designing new enterprise-level approaches to assurance for a set of businesses that are compliant with regulation and influential in the food chain.
3. Improving assurance of online food sales and identifying a series of interventions to improve safety for consumers buying food online

It is not guaranteed that all requirements will be commissioned through the call-off contract, the procurement route decision will be made on a case-by-case basis.

A. THE SPECIFICATION

Tenders are invited to supply resource to undertake the work described below providing strategic consultancy.

There is potential for the work to extend into other areas not yet identified. This will be defined as programme plans evolve across the whole of the FSA. However, as a guide the key objectives of the strategic partner will be to provide support including but not limited to:

Project & Programme Delivery Support:

- project initiation and support
- Provide planning support on specific projects.
- facilitating consultation/engagement activity
- business case – support development, review and evaluation of Business Cases and benefits etc
- Assist with clearly articulating the benefits of the programmes with both internal and external stakeholders.
- Define the target operating model options.
- Define programme measures for success.
- Support workstreams with high level strategic direction and guidance.
- Support Programme Board with decision making by providing guidance on design and implementation of new models, pilots and workstreams
- Discovery work to inform emerging projects within the programme, which may include gaining insight into specific business sectors, supporting LAs working in the online environment
- Research/analysis (either desk based or through engagement)
- Specialist analytics including socio-economic impact, and risk/benefit modelling and assessment

Organisation Design

- Assist with identifying business change activities,
- Carry out relevant business analysis and research to inform next steps
- Undertaking organisation design and capability reviews
- Process review / redesign and implementation
- Governance / reporting / performance management reviews
- Development of performance frameworks
- Strategic support to the future design of the FSA
- Other work to be determined in support of FSA strategic priorities

Programme Governance and Expectations:

Each Programme will have its own governance arrangements that will be defined in each work package.

Relevant Subject Matter Experts will provide support to the Strategic Partner to ensure access to relevant information required to deliver all programme objectives.

The strategic partner will:

- provide input to a comprehensive project delivery plan
- highlight to the programme manager at the earliest opportunity if there are any barriers to completing their agreed deliverables, as well as any necessary changes to the original mandate
- be responsible for the supporting the delivery of all workstreams within the programme structure. This support will ensure workstreams have an agreed focus and strategic direction and all policy related issues are addressed to avoid delay in delivery
- provide weekly highlight report including progress details
- ensure the programme team is aware of any key meetings with senior stakeholders.

Data Protection

Please outline in your tender how you will comply with the GDPR, recognising the commissioning authority's role as the 'data controller' and the contractor's role as the 'data processor', and responding to the sections below. If successful you may also be asked to carry out a Privacy Impact Assessment (PIA), and a privacy notice may be required, which will be reviewed by the FSA data security team.

Data security

Please confirm in your tender that you have in place, or that you will have in place by contract award, the human and technical resources to perform the contract to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects.

Please provide details of the technical facilities and measures (including systems and processes) you have in place, or will have in place by contract award, to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects. Your response should include, but should not be limited to facilities and measures:

- to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- to comply with the rights of data subjects in respect of receiving privacy information, and access, rectification, deletion and portability of personal data;
- to ensure that any consent-based processing meets standards of active, informed consent, and that such consents are recorded and auditable;
- to ensure legal safeguards are in place to legitimise transfers of personal data outside the EU (if such transfers will take place);
- to maintain records of personal data processing activities; and
- to regularly test, assess and evaluate the effectiveness of the above measures.'

Framework and Contracting

A Call off contract with the winning supplier acting as a strategic delivery partner for the FSA work programmes.

The call off contract will have a total capped value of £5,000,000 over the initial 2 year duration.

The FSA holds no commitment to the delivery of work packages under this call off agreement.

This tender is being advertised for further competition to suppliers on CCS Framework RM6187 Management Consultancy Framework Three (MCF3) Lot 2: Strategy & Policy.

Each Work Package will be called off by FSA by issuing the specification, deliverables and estimated timeline to allow the SDP to provide their technical and commercial response.

For the purposes of this Call Off Contract we will also be awarding the first work package, Work Package#1. This work package will also form the basis for the evaluation.

Work Package #1

Title: Preparation and Implementation of a Non-Departmental Public Body (NDPB) GovCo as a Contingency for the FSA Delivery of Official Controls Contracts.

Overview:

FSA are the central competent authority for the delivery of official controls in FSA approved establishments in England and Wales. These official controls are delivered through 6 geographical contracts by a single supplier.

Following the collapse of Carillion in 2018 which affected 450 public sector contracts, there is increased scrutiny across government contracts. Part of that scrutiny is around the development of contingency plans for supplier failure, particularly for single supplier delivery models.

Objective: FSA require a strategic delivery partner to support FSA in the preparation and implementation of a skeleton GovCo to allow the GovCo to step in should the supplier fail and maintain the delivery of the services.

To achieve the objectives the strategic partner will work with the Project Manager to produce the following DELIVERABLES:

	Deliverable Description	Expected Delivery Date
A	Produce a report that demonstrates that FSA meet the criteria for setting up a GovCo as a non-departmental public body (NDPB).	30/09/22
B	Clearly define the relationship between the GovCo and FSA in a way which supports the appropriate degree of delegation and independence of the GovCo, while providing assurance that financial management arrangements ensure propriety, regularity and value for money and that risks will be managed.	30/09/22
C	Produce a report demonstrating that the GovCo exhibits the characteristics of an Arm's Length Body (ALB) showing that alternative delivery models have been considered and provide evidence why they are not suitable.	30/09/22
D	Provide evidence to support funding method of GovCo – either Grant in Aid or Grant.	31/10/22
E	Provide evidence to support accounting standard that the GovCo will operate against – either FRem or FRS102	31/10/22
F	Produce the required documentation to test the proposal with the Treasury Classification Branch	31/10/22
G	Produce a shared services agreement between the FSA and the GovCo to include: Communications GDPR Estates Financial Arrangements Internal Audit IT equipment and support service provision Legal Security Funding and charging arrangements	30/11/22
H	Produce the required documentation to ask the Public Bodies Reform team to formally review the assumptions and categorise the GovCo.	30/11/22
I	Produce the Business Case for EMT, Cabinet Office and HMT approval	31/12/22

J	Produce a step-by-step list of activities, timings, and costs for running a dormant company	31/01/23
K	Produce a step-by-step list of activities, timings, and costs for activating a dormant company.	31/01/23

Requirement:

Demonstrate ability of setting up non departmental public body. Provide evidence and methodology for how you will deliver the key deliverables found within Work Package #1 including risk and risk mitigation.

Timeframes: 12th September 2022 to 31st January 2023.

FSA Resources:

The FSA will make available the following SMEs to assist in this review:

Project Manager
Commercial
Finance - for Charging, Payments and VAT
Legal
Operations Manager
HR

Cost:

Fixed cost for the planned work with optional increase for scope changes subject to pre-approval from FSA.

Subject to final approvals the expected budget will be in the region of £150k exc VAT.

B. PROCUREMENT TIMETABLE

Table 1 details an **estimated** project timetable for the project. Tenderers should however be aware that the Agency needs to acquire the evidence outlined in this ITT in a timely manner and you should justify your timings in your work plan.

TABLE 1. ESTIMATED PROJECT TIMETABLE	
EXPECTED DATE	INVITATION TO (ITT) TENDER
26th July 2022	Invitation to Tender (ITT) issued by the Agency
Immediately as above	ITT Clarification period opens*
12 noon 3rd August 2022	ITT Clarification period closes**
12 Noon, 22 nd August 2022	Closing date for submission of ITT responses***
W/c 22 August 2022	Evaluation of ITT responses
W/c 30th August 2022	Appraisal panel meeting held to consider clarified ITT responses
W/c 5 th September August 2022	Tenderers notified of outcome of appraisal and preferred Tenderer (or Tenderers) identified
W/c 5 th September 2022	Call Off Contract and Work Package 1 awarded and signed

12th September 2022	Project initiation meeting takes place and Work Package# 1 commences

* If a Tenderer wishes to raise any points of clarification over the procurement process, the actual project objectives or any other query these must be raised through the ECMS by the date specified.

** Queries will not be answered after this date.

*** Submissions must be uploaded onto the ECMS before the closing date and time.

Further Information

For any technical queries or issues regarding the use of ECMS please contact the eSourcing Helpdesk:

Phone: 0800 368 4850

Email: help@bravosolution.co.uk.

For any points of clarification regarding this specification or the FSA's procurement procedures please submit through ECMS.

Closing Date

Tenders should be submitted on ECMS **by the date specified on ECMS.**

Tenders received after this time will not be considered or evaluated. Please allow sufficient time to upload your tender and all supporting evidence before the closing date.

Notification of Submission of Tender

On successfully submitting your tender you should see a popup box appear on the screen indicating that your tender has been successfully submitted. In addition, you will receive an automatic email from ECMS with a reference code.

C. EVALUATION OF TENDERS

The award of the contract will be on the basis of the 'Most Economically Advantageous Tender' (MEAT).

The Tenderers Application consists of the:

- Technical envelope 80%, in which applicants should detail the approach, the work plan and their ability to undertake the work, and
- Commercial envelope 20%, in which applicants should outline all costs to conduct the proposed work, and

Any other relevant supporting information

Tenders will be evaluated by FSA evaluators using a numerical system. The table below shows weightings that have been allocated to each section of the application form and these used by the evaluators: -

TABLE 2. EVALUATION CRITERIA FOR SELECTION OF SUCCESSFUL TENDERER	
CRITERIA	PERCENTAGE WEIGHTINGS
TECHNICAL CRITERIA – 80%	Made up of
1. Delivery of the Requirements	35%

2. Organisational experience, expertise and staff capacity	10%
3. Project management including Risk Management	15%
4. Knowledge transfer	10%
5. Social value 6.1 Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce.	10%
COMMERCIAL CRITERIA – 20%	20%

Annex A – Technical Proposal



[illegible]

[illegible]



[Redacted content]

