

---

## **Call-Off Order Form for RM6187 Management Consultancy Framework Three (MCF3)**

---

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

### Order Form

Call-off reference: SR786491709

The buyer: HM Revenue & Customs

Buyer address: Stanley Street, Salford, M60 9HL

The supplier: McKinsey & Company, Inc. United Kingdom  
Supplier address: 100 Museum Street, London, WC1A 1PB  
Registration number: FC012665  
DUNS number: 294993308

### Applicable framework contract

This Order Form is for the provision of the Call-Off Deliverables and dated 29 November 2021.

It is issued under the Framework Contract with the reference number RM6187 for the provision of management consultancy services.

### Call-off lot: 3

### 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 cannot be used. If the documents conflict, the following order of precedence applies:

1. This Order Form including 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 5 (Corporate Social Responsibility)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)

- Joint Schedule 11 (Processing Data)

## **Call-Off Schedules**

- Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 3 (Continuous Improvement)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 18 (Background Checks)
  - Call-Off Schedule 20 (Call-Off Specification)
  - Call-Off Schedule 23 (HMRC Terms)
4. CCS Core Terms (version 3.0.10)
  5. Joint Schedule 5 (Corporate Social Responsibility)
  6. Call-Off Schedule 4 (Call-Off Tender)

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 Supplier shall comply with the Customer's Mandatory Terms as set out in Call Off Schedule 23. For the avoidance of doubt and contrary to any other provision relating to precedence of terms in this Call-Off Contract, in case of any ambiguity or conflict, the Customers Mandatory Terms will supersede any other terms in this Call Off Contract.

Special Term 2: This Call-Off Contract, and the work carried out in relation to it, shall be deemed a Tier 1 contract (following the Crown Commercial Service's Information Note 05/16 on "Open Book Contract Management" and the accompanying OBCM guidance) and accordingly the parties agree that the Customer's audit and inspection rights under (b)(c) and (h) within the definition of "Audit" in Joint Schedule 1 (Definitions) shall not apply.

Special Term 3: For the avoidance of doubt, the Supplier will not keep accurate records of time spent per consultant grade and will not make them available for inspection or invoicing purposes.

**Call-off start date: 15/11/2021**

**Call-off expiry date: 10/12/2021**

**Call-off initial period: 1 Month**

## **Call-off deliverables**

### **Framework Schedule 1 (Specification)**

Provision of objective advice on the portfolio of work which is multi-disciplinary and transformational. This is to include identification of options for consideration.

### Background and context

HMRC has taken real steps forward to transformation into a digital-forward tax authority over the last few years. However current programmes are long, and governance is often complex. This means space of delivering real change in service provision can be slow. The forced changes we had to implement since the start of the pandemic has demonstrated that faster change is achievable, and we want to build on the best of that experience to create a long-term architecture that can deliver rapid and ongoing service improvement.

### Objectives for the work

The initial 4–5-week project will have the following objectives:


1. Articulating the key elements of a model office capability, which can accelerate ongoing service transformation across HMRC
2. Designing the model office delivery vehicle which will be tested initially in CSG
3. Establishing a PAYE mobilisation plan within CSG, that lays the groundwork to start work at the start of 2022
4. Governance, reporting and resourcing for this effort

### Deliverables for the initial project

The deliverables for the areas led by the Supplier team will be:

1. An aligned, HMRC-wide articulation of a model office capability including objectives that HMRC is seeking to achieve; scope and solution space (i.e., CSG and CCG); an approach to design and delivery of changes; clear success criteria to be measured; and a top-down qualitative view of likely service candidates.
2. The solution design for the model office delivery vehicle, including the multiple components required to accelerate service digitisation. These will include the approach to service redesign; roles and skills needed to transform and then drive iterative improvement (including an understanding of culture and mindset-related aspects); IT expertise (including early view on future state of IT platforms); options for how this delivery vehicle could work within existing organisational structures in the Department. This may become the reference architecture for HMRC future work.
3. A high-level view on the value at stake in PAYE based on prior diagnostic work and the submission and outcome of SR (minimising new work on the current state); a roadmap covering a first stack of products; and an action plan and potential initial steps towards transforming the first candidate service, likely to be a priority product/service in PAYE (such as Tax Estimation Service, PAYE Repayment, P800 journey)

The principles associated with how the support will be provided, and the outcomes to be supported by the Supplier are set out in the Supplier Proposal



### **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: £99,000.00

### **Call-off charges**

Fixed Cost £99,000.00 (exclusive of VAT)

The Call-Off Contract Charges are on a fixed price basis (inclusive of all expenses)

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**

Not Applicable

### **Payment method**

Monthly invoices in arrears. PO transfer through the HMRC SAP Ariba Network

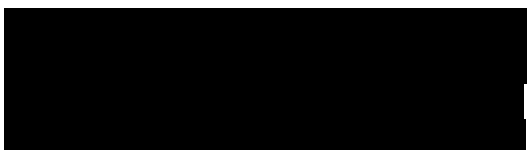
### **Buyer's invoice address**

Payments will be directed through the HMRC SAP Ariba Network

### **Buyer's authorised representative**



### **Supplier's contract manager**



**Buyer's security policy**

Appended at Call-Off Schedule 9

**Supplier's authorised representative**

[Redacted]

**Progress meeting frequency**

Weekly progress meetings on Fridays to commence on 12/11/2021. Further details are set out in the Supplier Proposal see Call-Off Schedule 4

**Key staff****Supplier**

[Redacted]

[Redacted]

[Redacted]

**Customer**

[Redacted]

[Redacted]

[Redacted]

**Key subcontractor(s)**

Not Applicable

## **Commercially sensitive information**

Supplier's Proposal (see Call-Off Schedule 4), Supplier pricing breakdowns, Supplier Background Intellectual Property Rights, Supplier personal data. Further context in joint schedule 5 (Commercially Sensitive Information)

## **Service credits**

Not Applicable

## **Additional insurances**

Not Applicable

## **Guarantee**

Not Applicable

## **Buyer's environmental and social value policy**

HMRC Sustainable Procurement Strategy available online at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/310632/HMRC\\_Sustainable\\_Procurement\\_Strategy.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/310632/HMRC_Sustainable_Procurement_Strategy.pdf)

HMRC complies with the requirements outlined in the Social Value Model, introduced under [PPN 06/20](#).

## **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: [REDACTED]

Name: [REDACTED]

Role: [REDACTED]

Date:

**For and on behalf of the Buyer:**

Signature: [REDACTED]

Name: [REDACTED]

Role: [REDACTED]

Date:



## Call-Off Schedule 4 (Call Off Tender)

Call Off Tender response and subsequent updates consist of the following embedded documents:

Suppliers Proposal

[REDACTED]

# 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):

<b>"Breach of Security"</b>	<p>1 the occurrence of:</p> <ul style="list-style-type: none"><li>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/or</li><li>b) 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,</li></ul> <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>
<b>"Security Management Plan"</b>	<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 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.

## **ANNEX 1 - SECURITY MANAGEMENT PLAN**

Security Management Plan as embedded below:

