Crown
Commercial
Service

Call Off Order Form for Management Consultancy Services

SECTION A

This Call Off Order Form is issued in accordance with the provisions of the Framework Agreement for the provision of Audit Services RM3745 Lot 3 dated 4th September 2017

The Supplier agrees to supply the Services specified below on and subject to the terms of this Call Off Contract.

For the avoidance of doubt this Call Off Contract consists of the terms set out in this Call Off Order Form and the Call Off Terms.

Order Number	**TBC**
From	**HM Revenue & Customs (HMRC) ("CUSTOMER")**
To	**KPMG LLP ("SUPPLIER")**

SECTION B

CALL OFF CONTRACT PERIOD

1.1.	**Commencement Date**: 31 July 2020
	Expiry Date: 30 November 2020 End date of Initial Period: Not Applicable End date of Extension Period Not Applicable Minimum written notice to Supplier in respect of extension: Not Applicable

SERVICES

2.1.	**Services required**: Provision of 20 days support to provide advice and delivery of work to support the completion of an internal audit review of Cloud Transition (including Cloud Security). There are several areas of support required as set out below: [redacted]

PROJECT PLAN

3.1.	**Project Plan**: Not applied

CONTRACT PERFORMANCE

4.1.	**Standards**: Applicable standards for this contract are per Clause 11 (Standards) detailed in the Call-off terms for RM3745 which can be accessed via the CCS website.
4.2	**Service Levels/Service Credits**: Not applied
4.3	**Critical Service Level Failure**: Not applied
4.4	**Performance Monitoring:** Not applied
4.5	**Period for providing Rectification Plan:** In Clause 39.2.1(a) of the Call-off terms for RM3745 which can be accessed via the CCS website.

PERSONNEL

5.1	**Key Personnel**: As per Section 27, Key Personnel, detailed in the Call-off terms for RM3745 which can be accessed via the CCS website. The key KPMG contact for this assignment is [redacted]
5.2	**Relevant Convictions** Clause 28.2 of the Call-off terms for RM3745 which can be accessed via the CCS website.

PAYMENT

6.1	**Call Off Contract Charges** (including any applicable discount(s), but excluding VAT): In Annex 1 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing) The fixed contract value for the provision of advice and delivery of work to support the completion of an internal audit review of Cloud Transition (including Cloud Security) is £29,100 (exclusive of VAT which will be charged at the then prevailing rate). The 20 days support requested by the Customer is expected to be provided by the Supplier as follows. [redacted]
6.2	**Payment terms/profile** (including method of payment e.g. Government Procurement Card (GPC) or BACS):

	In Annex 2 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing) The payment method for this Call-Off Contract is by BACS transfer through the HMRC Ariba network. The Supplier will issue an electronic invoice. The Customer will pay the Supplier within 30 days of receipt of a valid invoice.
6.3	**Reimbursable Expenses**: Not permitted
6.4	**Customer billing address** (paragraph 7.6 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)): The Supplier will issue an electronic invoice via the HMRC Ariba Network
6.5	**Call Off Contract Charges fixed for** (paragraph 8.2 of Schedule 3 (Call Off Contract Charges, Payment and Invoicing)): Call Off Contract Charges are fixed for the Contract term.
6.6	**Supplier periodic assessment of Call Off Contract Charges** (paragraph 9.2 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)) will be carried out on: Not applicable
6.7	**Supplier request for increase in the Call Off Contract Charges** (paragraph 10 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)): Not permitted

LIABILITY AND INSURANCE

7.1	**Estimated Year 1 Call Off Contract Charges**: The fixed sum of £29,100 (exclusive of VAT which will be charged at the then prevailing rate).
7.2	**Supplier's limitation of Liability** (Clause 37.2.1 of the Call Off Terms); Subject to Clause 37.1 and 37.3, Supplier's total aggregrate liability (whether expressed as an indemnity or otherwise) in respect of all the Losses incurred by the Customer under or in connection with this Call Off Contract (whether under common law or statute, tort (including negligence), breach of statutory duty or otherwise) shall in no event exceed one hundred and twenty five percent (125%) of the charges paid nor payable to the Customer during the Call-Off contract period. Not withstanding anything to the contrary set forth in the Call Off Contract, the Parties agree and acknowledge that, the Supplier's maximum aggregate liability to the Customer (including for any liability for acts or omissions of its Supplier Personnel) under or in relation to the Call Off Contract (whether in contract, tort, negligence, indemnity, strict liability in tort, by statute or otherwise) for any and all claims, to the extent caused by the Supplier, arising in respect of: a) any breach of the terms of Clause 35.5 (Protection of Personal Data), b) Personal Data c) any fines and/or penalties imposed pursuant to Data Protection Legislation shall be capped in (aggregate) at 125% of the total Charges paid or payable to the Customer during the Call-Off contract Period.
7.3	**Insurance** (Clause 38.3 of the Call Off Terms):

	Applicable insurance terms are available in Clause 38.3 of the Call-off terms for RM3745 which can be accessed via the CCS website.

TERMINATION AND EXIT

8.1	**Termination on material Default** In Clause 42.2.1(c) of the Call-off terms
8.2	**Termination without cause notice period** In Clause 42.7.1 of the Call-off terms
8.3	**Undisputed Sums Limit**: In Clause 42.7 of the Call-off terms
8.4	**Exit Management:** Under the terms of the Contract, the Supplier must commit to co-operating with the customer to ensure efficient Exit Management. The Supplier must ensure that knowledge transfer to the Customer's team is a fundamental part of the Exit Management process.

SUPPLIER INFORMATION

9.1	**Supplier's inspection of Sites, Customer Property and Customer Assets:** Not applicable
9.2	**Commercially Sensitive Information**: During the conduct of this work, the contractor may see or be provided Commercially Sensitive information. In this event they must keep the information secure, not passed on to other colleagues not involved in the review and held on the HMRC network.

OTHER CALL OFF REQUIREMENTS

10.1	**Recitals** (in preamble to the Call Off Terms): Refer to the preamble of the Call Off Terms for RM3745 which can be accessed via the CCS website. Recital A
10.2	**Call Off Guarantee (Clause 4 of the Call Off Terms):** Not required
10.3	**Security**: Short form security requirements

	And Security Management Plan as embedded below and provided as Appendix B at the end of this Order Form in the signed DocuSign version of this contract.  Security Plan_24072020_KPM(
10.4	**ICT Policy:** The Supplier's team must ensure that when they are using equipment provided by the Customer to access Customer's systems they comply with the Customer's ICT/Security policies which can be located at the following URL: https://intranet.prod.dop.corp.hmrc.gov.uk/section/how-do-i/get-help-security/security-information-zone The Supplier must ensure that all team members are made aware of the need to comply with ICT/Security policies and that team members are directed to where the security policies are located.
10.5	**Testing**: Not applied
10.6	**Business Continuity & Disaster Recovery**: Not applied
10.7	NOT USED
10.8	**Protection of Customer Data** It is not envisaged that this contract will involve the processing of Customer Data, but should this arise then Clause 35.2.3 Call-off terms for RM3745 which can be accessed via the CCS website will apply
10.9	**Notices** (Clause 56.6 of the Call Off Terms): Customer's postal address and email address: HMRC Commercial Directorate 5W Ralli Quays 3 Stanley Street Salford M60 9LA [redacted] Supplier's postal address and email address: KPMG LLP 15 Canada Square, London, E14 5GL [redacted]
10.10	**Transparency Reports** In Call Off Schedule 13 (Transparency Reports) Not applied
10.11	**Alternative and/or additional provisions (including any Alternative and/or Additional Clauses under Call Off Schedule 14 and if required, any Customer alternative pricing mechanism):**

Customer's additional Clauses will apply as provided in Appendix A.

Other additional Clauses are as follows.

1. Deliverables

The Customer shall not:

• attribute any Deliverables to the Supplier; or

• make reference to the Supplier's role in the provision of the Deliverables or the Services;

in each case without the Supplier's prior written consent.

2. Impact of Covid-19

The timing of the Services and its performance will be dependent on all relevant information and documentation and access to personnel being made available to the Supplier promptly as and when required by the project timetable. Supplier shall use all reasonable endeavours to meet any agreed timetable. If any stakeholder or member of either team is unavailable for an extended period of time due to sickness or measures taken to control the spread of illness, there may be a delay or temporary cessation in the delivery of the Services and the Supplier will work with the Customer to mitigate any impact.

In the provisions below, references to 'we' and 'us' means the Supplier, and references to 'you' means the Customer.

3. Responsibilities of management

3(a) While we may comment on processes and control procedures, the decision on whether those processes and control procedures may provide adequate assurance for your business needs shall rest with you in the light of your assessment of the risks facing your business. Where we make recommendations we shall take account of our view of good practice at the time we undertook the work but they shall reflect what we believe is practical and appropriate in the circumstances. It shall be for you to determine the extent to which our findings and recommendations may be suitable for your purposes and to assess our findings and recommendations in the light of the facts which we report and your knowledge of the business before you decide to implement any control changes. Because of the inherent limitations of any control structure, errors and irregularities may exist and may not be detected by us. Accordingly, our findings and recommendations shall be based on the evidence obtained by us which must be considered as persuasive rather than conclusive.

3(b)The responsibility for the prevention and detection of fraud and irregularities rests and shall rest with you. We shall report to you on such risk areas as we identify but the Services cannot be relied upon to identify all such areas nor to disclose all fraud or irregularities which may exist. Our detailed testing of transactions shall not be designed to detect fraud and irregularities.

3(c) The sole purpose of our work shall be to provide information to management. Accordingly, only your management may rely on any element of any deliverables provided by us to you. We consent now to the disclosure of any deliverables (but not any draft

	deliverables) provided by us to any of your employees who are required to have access to our deliverables for the proper performance of their duties and, subject to clause 4 below, to your external auditors. Save for these exceptions you shall not make reference to us having conducted any Internal Audit services on your behalf or represent that we have expressed any opinion as to the adequacy, reliability and effectiveness of internal controls that have been established by you. **4. External auditors** 4(a) You shall be entitled to provide a copy of any deliverables prepared by us, in whole but not in part, to your external auditors, provided that you communicate to your external auditors that: ■ where the deliverable is in draft, it has not been finalised and is subject to change as our work progresses; ■ the deliverable concerned will have been prepared for the sole purpose of our providing information to management in accordance with the Call Off Contract; ■ there will have been particular features of our work determined by your needs at the time which may not be appropriate for their needs; ■ the provision of any such deliverable (including any information, explanations and working papers which we may subsequently provide at our sole discretion) should not be regarded as suitable for use by them or for any other purpose; ■ should they choose to rely on any such deliverable (including any information, explanations and working papers which we may subsequently provide at our sole discretion) they shall do so at their own risk; and ■ we shall accept no responsibility or liability to your external auditors in connection with any such deliverable. 4(b) We shall consider any request that you may make for us to meet your external auditors and to provide information explanations and working papers which support any deliverable issued by us and to which your external auditors may have gained access pursuant to these Additional Terms, on condition that we may, at our sole discretion, require your external auditors to enter into an agreement with us in the form which we determine before so doing. 4(c) In the particular circumstances of the Services, neither we nor any of our partners or directors, employees and agents, together with any other body associated with us nor each and all of their partners, directors, employees and agents shall have any liability to you or to any other beneficiary of the Services, in contract or tort or under statute or otherwise, for any loss or damage suffered or costs incurred by you (or by any such other party) arising from or in connection with the provision of any deliverable issued by us to your external auditors (including any information explanations and working papers which we may subsequently provide), however the loss or damage is caused, including if caused by our negligence but not if caused by our fraud or other deliberate breach of duty. This

	exclusion shall not operate to exclude any liability which cannot lawfully be limited or excluded. **5. Survival on termination** The following clauses of these Additional Terms shall survive expiry or termination of the Call Off Contract: clauses 1, 2, 3(a), (b) and (c), and 4 (a), (b) and (c), and this clause 5. **6. Critical comments** In addition, nothing in the contract (including clause 27) will prevent KPMG from making critical comments in any internal audit reports regarding the client, if appropriate in light of our findings from individual reviews. **7. Rights of other Contracting Authorities** If you wish us to owe a duty of care to other Contracting Authorities, please let us know so that their treatment as Customer can be made clear in the Call Off Contract and our work plan adjusted to address their requirements. **8. The Way We Work** You will inform us promptly if information or developments come to your attention which might have a bearing on our work and you will promptly provide us with all information and assistance and access to documentation and personnel that we reasonably require (and if outside your immediate control you will use reasonable endeavours to obtain these for us). You are responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the organisation. You are responsible for risk management arrangements in the organisation. The identification and prioritisation of risks and the strategies put in place to deal with identified risks remain your sole responsibility.
10.12	**Call Off Tender**: Not applied
10.13	**Publicity and Branding (Clause 36.3.2 of the Call Off Terms)** Clause 36.3.2 of the Call-off terms for RM3745 which can be accessed via the CCS website.
10.14	**Staff Transfer** Annex to Call Off Schedule 10, List of Notified Sub-Contractors (Call Off Tender). Not applied
10.15	**Processing Data** Not applied

FORMATION OF CALL OFF CONTRACT

BY SIGNING AND RETURNING THIS CALL OFF ORDER FORM (which may be done by electronic means) the Supplier agrees to enter a Call Off Contract with the Customer to provide the Services in accordance with the terms 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.

In accordance with paragraph 7 of Framework Schedule 5 (Call Off Procedure), the Parties hereby acknowledge and agree that this Call Off Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of the Call Off Order Form from the Supplier within two (2) Working Days from such receipt.

For and on behalf of the Supplier:

Name and Title	[redacted]
Signature	[redacted]
Date	

For and on behalf of the Customer:

Name and Title	[redacted]
Signature	[redacted]
Date	

APPENDIX A

Authoritory's Mandatory Terms

A. For the avoidance of doubt, references to 'the Agreement' mean the attached Call-Off Contract between the Supplier and the Authority. References to 'the Authority' mean 'the Buyer' (the Commissioners for Her Majesty's Revenue and Customs).

B. The Agreement incorporates the Authority's mandatory terms set out in this Schedule 12

C. In case of any ambiguity or conflict, the Authority's mandatory terms in this Schedule 12 will supersede any other terms in the Agreement.

1. Definitions

"Affiliate"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Authority Data"	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Authority; and/or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;
"Charges"	the charges for the Services as specified in "Call-Off Contract Charges and Payment".
"Connected Company"	means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;
"Control"	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;
"Controller", "Processor", "Data Subject",	take the meaning given in the GDPR;
"Data Protection Legislation"	(a) the GDPR, the Law Enforcement Directive (Directive EU 2016/680) and any applicable national implementing Laws as amended from time to time; (b) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; (c) all applicable Law about the processing of personal data and privacy;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"Key Subcontractor"	any Subcontractor:

	(a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract;
"Law"	any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Personal Data"	has the meaning given in the GDPR;
"Purchase Order Number"	the Authority's unique number relating to the supply of the Services;
"Services"	the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods;
"Subcontract"	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
"Subcontractor"	any third party with whom: (a) the Supplier enters into a Subcontract; or (b) a third party under (a) above enters into a Subcontract, or the servants or agents of that third party;
"Supplier Personnel"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement;
"Supporting Documentation"	sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice;
"Tax"	(a) all forms of tax whether direct or indirect; (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions.

levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and

(d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above,

in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;

"Tax Non-Compliance"	where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1, where: (a) the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and (b) any "Essential Subcontractor" means any Key Subcontractor;
"VAT"	value added tax as provided for in the Value Added Tax Act 1994.

2. Payment and Recovery of Sums Due

2.1 The Supplier shall invoice the Authority as specified in "Call-Off Contract Charges and Payment" section of the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

2.1.1 the Supplier does so at its own risk; and

2.1.2 the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

2.2 Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority's electronic transaction system.

2.3 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

3. Warranties

3.1 The Supplier represents and warrants that:

3.1.1 in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;

3.1.2 it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

3.1.3 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue and the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.

3.2 If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.

3.3 In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4. Promoting Tax Compliance

4.1 All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.

4.2 To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

4.3 The Supplier shall provide to the Authority the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.

4.4 If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:

4.4.1 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

4.4.2 promptly provide to the Authority:

(a) details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.

4.5 The Supplier shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 4.5 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

4.6 Upon the Authority's request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

4.7 If the Supplier:

4.7.1 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this may be a material breach of the Agreement;

4.7.2 fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or

4.7.3 fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

4.8 The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.

5. Use of Off-shore Tax Structures

5.1 Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract (**"Prohibited Transactions"**). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business.

5.2 The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.

5.3 In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.

5.4 Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that

provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

6 Data Protection and off-shoring

6.1 The Processor shall, in relation to any Personal Data processed in connection with its obligations under the Agreement:

6.1.1 not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) 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

(d) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

6.2 Failure by the Processor to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

7 Commissioners for Revenue and Customs Act 2005 and related Legislation

7.1 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ('CRCA') to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 19 of CRCA.

7.2 The Supplier shall comply with, and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

7.3 The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

7.4 The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.

7.5 In the event that the Supplier or the Supplier Personnel fail to comply with this Clause 7, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1. There is a person or entity which is either: ("X")

1) The Economic Operator or Essential Subcontractor (EOS)

2) Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1];

3) Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2. X has been engaged in one or more of the following:

a. Fraudulent evasion[2];

b. Conduct caught by the General Anti-Abuse Rule[3];

c. Conduct caught by the Halifax Abuse principle[4];

d. Entered into arrangements caught by a DOTAS or VADR scheme[5];

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10

[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

[4] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

[5] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

e. Conduct caught by a recognised 'anti-avoidance rule'[6] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

f. Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];

g. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

i. In respect of (a), either X:

1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[8]; or,

2. Has been charged with an offence of fraudulent evasion.

ii. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

iii. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

iv. In respect of (f) this condition is satisfied without any further steps being taken.

v. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

[6] The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

[7] Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight

[8] The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

Annex 2 Form

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: [for Supplier to insert Contract reference number and contract date] ('the Agreement')

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.

2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

SIGNED:
FULL NAME:
POSITION:
COMPANY:
DATE OF SIGNITURE:

APPENDIX A

SECURITY MANAGEMENT PLAN

Background

The Contractor is required to prepare a Security Plan in accordance with HMRC's Security Policy.
The requirements set out in this Security Plan also apply to any sub-contractors engaged by the Contractor to perform any of the services under the Contract.
HMRC has developed a standard set of questions and recommendations (see attached Appendices) to ensure consistency across relevant contracts.
The Contractor is required to provide answers to the standard set of questions contained within this questionnaire to formulate the initial Security Plan.
This Security Questionnaire covers the principles of protective security to be applied in delivering the services in accordance with HMRC's Security Policy and Standards
The Contractor's response to this questionnaire, with any subsequent amendments as may be agreed as part of a clarification process, will be included in the signed version of any resulting agreement, as confirmation that the content of the Security Plan has been agreed with HMRC.

1 Policy & Standards

1a Please confirm that you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.

Yes

1b Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from Security Policy Framework and any Security Requirements recorded in the schedules and/or Order Form.

KPMG complies with the requirements of the Government's Security Policy Framework, and has extensive experience of applying client requirements for the handling of Government Information.

1c If you believe that the Public Sector Network (PSN) Code of Connection, available from www.gov.uk, will apply to your organisation and any subcontractors, please provide details of how you will conform to this. **N/A**

1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the General Data Protection Regulation see GDPR and in accordance with Clause 23 (*Protection of Personal Data*) of the Contract. **In our role as a trusted professional services provider, KPMG is dedicated to protecting the privacy and confidentiality of information entrusted to us. We comply with the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 ('the data protection legislation'). KPMG has also produced internal guidance on the handling of Government Information, which is in accordance with the Security Policy Framework. This is issued to personnel to supplement any guidance provided by clients.**
1e Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found here **Yes, KPMG LLP is registered with the ICO and the reference number is Z7047609. The ICO registration certificate is available if required.**

1f Please provide details of any security accreditation that your organisation currently possess, such as but not exclusive to, ISO27001 and PCI DSS and describe the process used to achieve the accreditation. **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIALSENSITIVE. KPMG UK has held ISO 27001 certification since 2002. As part of our ISO 27001 certification, we are independently audited at 6 monthly intervals by an external accreditation body. Our key information security controls are also subject to annual audit by KPMG International. In addition, KPMG holds the Cyber Essentials certificate. Note: for confidentiality reasons, we cannot provide results of audit activity.**
1g If you intend to involve sub-contractors at any stage during the Contract please list them and provide details of how you will ensure their compliance with all aspects of this Security Plan. **No sub-contractors will be used on this review**
1h As appended to this Schedule 2.4, Appendix G, Security Aspects Record, defines the Government Security Classifications (see Government Security Classifications) carried by the HMRC data. If you are successful in the tender process, you will require a Security Manager (or appointed person), to take responsibility for the security of the data. Please provide the name of your Security Manager who will act as a first point of contact and conduct ongoing management of security risks and incidents (including identification, managing, and reporting in line with agreed procedures for actual or suspected security breaches). **Andrew North, Director.**
2 Physical Security (For requirements please see Appendix A – Physical Security)

2a For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls. **All work to be conducted off-site and remotely largely at staff home premises due to current working arrangements.**
2b Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding HMRC assets. Detail measures such as construction of buildings used for handling HMRC assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls. **All work to be conducted off-site and remotely largely at staff home premises due to current working arrangements.**
3 IT Security (For requirements please see Appendix B – IT Security) Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed. If no assessment has been performed please answer all questions in this section.

3a Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed. If no assessment has been performed please state when you expect it to be completed. **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIAL-SENSITIVE. KPMG is ISO27001 accredited and also holds Cyber Essentials Plus certification.**
3b Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention) and how regularly you update them. **Our work will be conducted on HMRC infrastructure using HMRC laptops.** **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIAL-SENSITIVE. KPMG is ISO27001 accredited and also holds Cyber Essentials Plus certification.**
3c Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users. **Our work will be conducted on HMRC infrastructure using HMRC laptops.** **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIAL-SENSITIVE. KPMG is ISO27001 accredited and also holds Cyber Essentials Plus certification.**

3d Please provide details of how your security and access control policy complies with the Security Policy Framework including where necessary, use and control of back-up systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets. **Our work will be conducted on HMRC infrastructure using HMRC laptops.** **KPMG complies with the requirements of the Government's Security Policy Framework, and has extensive experience of applying client requirements for the handling of Government Information.**
3e Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing). **Our work will be conducted on HMRC infrastructure using HMRC laptops.** **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIAL-SENSITIVE. KPMG is ISO27001 accredited and also holds Cyber Essentials Plus certification.**
3f Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data. **Our work will be conducted on HMRC infrastructure using HMRC laptops.** **The KPMG IT network has been self accredited to operate at OFFICIAL and with additional encryption can operate at OFFICIAL-SENSITIVE. KPMG is ISO27001 accredited and also holds Cyber Essentials Plus certification.**

3g Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned and how all data will be rendered unreadable and irretrievable in line with the Security Policy Framework. **Our work will be conducted on HMRC infrastructure using HMRC laptops.**
4 Personnel Security (For requirements please see Appendix C – Personnel Security)
4a Have all staff who will have access to, or come in to contact with HMRC data or assets undergone Baseline Personnel Security Standard checks (See www.gov.uk for further information). **Yes.**
4b Please provide details of how you will ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract? **For this work we will have an Information Protection Plan (IPP) in place which all staff will be asked to read and sign.**

4c All contractor's personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC's Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested. **Yes.**
5 Process Security (For requirements please see Appendix D – Process Security)
5a Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed. **For this review, all KPMG work will be carried out on HMRC provided hardware.**
5b Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration. **No third parties involved.**
5c Please confirm that you understand that HMRC Data must not be processed or stored outside the United Kingdom without the express permission of HMRC. **Yes. For this review, all KPMG work will be carried out on HMRC provided hardware.** If you are considering storing data outside of the UK, please provide details on how and where the data will be stored and also provide details of how you comply with Cabinet Office policy for offshoring see Offshoring **Not Applicable.**
5d In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent. **For this review, all KPMG work will be carried out on HMRC provided hardware and subject to HMRC security protocols. However, KPMG complies with the requirements of the Government's Security Policy Framework, and has extensive experience of applying client requirements for the handling of Government Information.**
5e What arrangements are in place for secure disposal of HMRC assets once no longer required? **For this review, all KPMG work will be carried out on HMRC provided hardware. KPMG complies with the requirements of the Government's Security Policy Framework, and has extensive experience of applying client requirements for the handling of Government Information.**
5f How will you immediately advise HMRC of security incidents that impact HMRC assets? **HMRC will be advised immediately by KPMG in the event of an IT security event impacting on HMRC provided laptops.**
6 Business Continuity (For requirements please see Appendix E – Business Continuity)

6a Please provide an overview of your organisation's business continuity and disaster recovery plans in terms of the HMRC data under the Contract, or attach a copy of your Business Continuity Plan. **The KPMG business continuity team follow the business continuity institute best practice guidelines and comply with ISO22301 as confirmed by independent internal audit. The firm has ISO27001 accreditation, the scope of external audit which includes business continuity management across the UK firm. If required we can provide this for incident and crisis management, business recovery planning and risk and impact mitigation.**
7 Cryptography
7a Will you be using commercial cryptography as part of this contract? If so, please provide details. **No**

The following appendices provide additional information on the types of security control that <u>may</u> be expected as a minimum for the protection of HMRC information, data and assets.

It is not a legally binding document, nor does it provide a definitive list of baseline security controls, and must be read in conjunction with HMG and HMRC Security Policy and Standards.

Appendix A – Physical Security

Please consider: the effect of topographic features and landscaping on perimeter security; the possibility of being overlooked; the ease of access and communications; the existence and proximity of public rights of way and neighbouring buildings; the existence of emergency and evacuation routes from adjacent buildings; the implications of shared accommodation; the location of police and emergency services; the build of the structure.

Building Security - There should be as few points of exit and entry as possible but in line with Health & Safety and Fire Regulations. Where exit and entry points exist then physical security controls, such as window bars, grilles shutters Security Doors etc may be installed. The effectiveness of these protection measures may be enhanced by the use of Intruder Detection Systems (IDS), CCTV or Guard Service.

Physical Security	Requirements	Recommended
Physical Access - secure areas	Visitors should be identifiable and escorted at all times	Visitors to be issued with identifying badges upon arrival. A visitor log maintained and visitors sign-in and out.

Building	Should be constructed of robust building materials typically, brick or lightweight block walls. External doors should be of solid construction and locked during silent hours. Access to keys should be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders should be maintained. The number of keys to a lock should be kept to a minimum. Spare keys should not be held in the same container as 'working keys'. The premises must be locked during 'silent hours' and keys secured.	Lockable double glazed or similar unit. Emergency exit doors included on intruder detection system. Security Keys should not be removed from the premises. Intruder alarm with keyholder response.
Environmental	Fire risk assessment should be carried out. Uninterruptible power supply for security and health & safety equipment.	Smoke detection system e.g. VESDA.
Transport and Storage	Adequate lockable storage for HMRC material. Material transported using processes agreed with HMRC.	Point to point transport of material in locked containers.

Appendix B – IT Security

IT Security	Requirements	Recommended
Cyber Essentials	It is a requirement for HMG suppliers to have undertaken selfassessment and achieved the Government backed Cyber Essentials scheme.	Cyber Essentials Plus with independent assessment and certification.
Authorisation	Users and Administrators must be authorised to use the System/Service.	

Authentication[9]	Individual passwords must be used to maintain accountability; Robust passwords should be used that are designed to resist machine based attacks as well as more basic guessing attacks. Passwords must be stored in an encrypted form using a one-way hashing algorithm. Passwords must be able to be changed by the end user, if there is suspicion of compromise. Passwords must be changed at least every 3 months.	Machine generated passwords. Multi-factor authentication should be considered for exposed environments and remote access. Passwords for privileged accounts/users (Administrators) etc. should be changed more frequently than every 3 months.
Access Control	Access rights to HMRC information assets must be revoked on termination of employment. Audit logs for access management in place showing a minimum of 30 days of activity.	
Malware Protection[10]	Controls such as anti-virus software must detect and prevent infection by known malicious code.[11] AV Administrators and users should be trained on use of AV software. Users should receive awareness training so that they are aware of the risks posed by malicious code from the use of email and	Consideration should be given to allowing privilege users (System Administrators) to only use a limited 'non-privilege role' to conduct vulnerable operations such as browsing or importing via removable media. Dual layered malware protection and detection capability.

[9] Authentication is the process by which people "prove" to the system that they are the person they claim to be. There are three possible authentication factors: Passwords (something a person knows), tokens (something a person possesses), and biometrics (something a person inherently is or how they behave).

[10] CESG Good Practice Guide No 7 provides information on the threats and vulnerabilities and risks associated with malicious code and also provides guidance on appropriate risk management measures.

[11] Heuristic scanning capabilities can help detect against previously undocumented attacks but AV products are generally ineffective against day zero attacks and are therefore only effective against known malicious code attacks. It is important therefore that systems and applications are locked down, patched against known vulnerabilities that could allow execution of malicious code e.g. in browsers and email clients.

	attachments, internet and removable media (CD, DVD, USB devices etc). Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality. File types should be limited. System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction. All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code. Application code development should be tightly controlled and subject to strict quality control to reduce the potential for insertion of backdoors that could be exploited by an attacker. For systems attaching to HMRC network, dual layered malware protection and detection capability.	
Network Security	Boundary controls that have a content checking and blocking policy in place e.g. firewalls.	Dual paired firewalls, different vendors. Anomaly detection capability e.g. Network intruder detection system.
Patch Management	Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality. File types should be limited. All Critical security patches should be deployed timeously and in line with vendor recommendations. The deployment of Important i.e. less critical patches should be deployed on the basis of risk.	

System Documentation	System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.	
Disposal of media	HMRC information assets must be sanitised in line with the Security Policy Framework in an agreed process with HMRC.	
Technical Testing	IT health check aka penetration testing for front facing internet services delivered to HMRC.	Consideration for regular IT health check of application and infrastructure services delivered to HMRC.
Use of Laptops and removable recordable media.	Laptops holding any information supplied or generated as a consequence of a Contract with HMRC must have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed. Approval from HMRC must be obtained before information assets are placed on removable media[12]. This approval must be documented sufficiently to establish an audit trail of responsibility. All removable media containing information assets must be encrypted. The level of encryption to be applied is determined by the highest HM Government Security Classification of an individual record on the removable media. Unencrypted media containing HMRC information assets must not be taken outside secure locations; the use of unencrypted media to store HMRC information assets must be approved by HMRC.	

Appendix C – Personnel Security

Personnel Security	Requirements	Recommended
Pre-employment checks	Pre-employment checks should meet the Baseline Personnel Security Standard (BPSS) and must be completed for all staff with potential or actual access to HMRC assets.	See www.gov.uk, specifically Disclosure & Barring Service for more information.

[12] The term drives includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media and external hard drives.

Confidentiality Agreements	Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested.	HMRC's Commercial Directorate can supply the template form.

Appendix D – Process Security

Process Security	Requirements	Recommended
Security Policies, Processes and Procedures	Procedures to be in place to determine whether any compromise of HMRC assets e.g. loss or modification of information, software and hardware has occurred. Procedures for the handling and storage of HMRC information assets should be established to protect from unauthorised disclosure and/or misuse. End of day procedures should ensure that HMRC assets are adequately protected from unauthorised access. A clear desk policy should be enforced. Procedures must be in place to ensure the HMRC's assets are segregated from any other Client's assets held by the contractor. Procedures for the secure disposal of the HMRC's assets must be in place. A challenge culture should be fostered, so that unknown staff or visitors are challenged. Where an access control system is used tailgating should be discouraged.	Assets, especially information assets must be destroyed when no longer required so that they cannot be reconstituted or reused by an unauthorised third party. Shedding is recommended. Electronic files should be weeded and deleted when no longer required.

Transfer of HMRC Data	Any proposed transfer of HMRC data must be approved by HMRC in writing. If the Contractor is unsure whether approval has been given, the data transfer must not proceed. Where data transfers are necessary in the performance of the Contract, they should be made by automated electronic secure transmission via the Government Secure Internet (GSI) with the appropriate level of security control. Individual data records (unless as part of a bulk transfer of an anonymised respondent survey data) will require specific transfer arrangements. Transfer of aggregated data such as results, presentations, draft and final reports may also need discussion and agreement, again in advance of any such transfer.	**Whenever possible, putting data on to removable media should be avoided.** Where this is unavoidable, hard drives and personal digital assistants, CD-ROM/DVD/floppy/USB sticks are only to be used after discussion and agreement with HMRC in advance of any such transfer. If the use of removable media is approved, data must be written to them in a secure, centralised environment and be encrypted to HMRC's standards. If you anticipate transferring data on removable media during the delivery of this project please set out your proposed transfer procedures.
Incident Management	Arrangements should be in place for reporting security breaches to the asset owner.	

Appendix E – Business Continuity

Business Continuity Requirements	Requirements	Recommended
Business Continuity Management	3rd party suppliers should provide HMRC with clear evidence of the effectiveness of its Business Continuity management arrangements and alignment with recognised industry standards, by assessing risks to their operations and producing and maintaining business continuity documentation	

Appendix F – Cryptography

	Requirements	Recommended

Commercial Cryptography	Where you intend to use commercial cryptography as a layer of security for HMRC data at rest or during processing please provide details of the product you intend using and confirmation of appropriate licencing.	

Schedule 2.4 – Appendix G – Security Aspects Record

G.1. This contract will involve the Contractor holding UK Government security classified material. It is a condition of this contract that this material must be protected. The standard of protection required is detailed below and varies with the level of security classification. Material passed to the Contractor will bear the security classification appropriate to it.

G.2 In determining the Security Classification 'Aggregated Material' has been considered. 'Aggregation' is the term used to describe the situation when a large number of data items at one classification are collected together. The impact of the compromise of the whole collection can often be significantly higher than the Impact of compromise of one item. This applies to compromises of Confidentiality, Integrity and Availability.

G. 3 To assist the Contractor in allocating any necessary classification to material which the Contractor may produce during the course of the contract and thus enable the Contractor to provide the appropriate degree of protection to it, this schedule formally advises you of the correct security classification to apply to the various aspects of the contract.

G.4 The highest security classification of the information with which the Contractor operates under this contract is OFFICIAL - SENSITIVE

G.5 The aspects of the contract which require a Security Classification are:-

Aspect	Security Classification

(provide full and detailed information)	

G.6 If the contract contains a Condition of Clause referring to “Secret Matter” this Secret matter is defined as the Aspects listed above.

G.7 The Contractor is responsible for ensuring that the level of protective marking associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this contract, that they are fully understood, and that the required security controls in the contract security conditions can and will be taken to safeguard the material concerned.

G.8 At the outset of this contract the person identified by the Contractor who will take responsibility for the security of the classified material:

Name: Role:

G.9 If during the term of the contract the person responsible for the security of the classified material changes, then the Contractor must advise the Client at the earliest opportunity.