Service Order

HM REVENUE & CUSTOMS SERVICE ORDER	
A1.	**HMRC Information** **Purchase Order to be issued under separate cover**
CD Reference:	SR1201952481
Purchase / Limit Order No	To be confirmed
HMRC Commercial Contact	
Name:	Fintan Bradley
Contact Telephone No.:	0300 051 9832
email:	fintan.bradley@hmrc.gov.uk
HMRC Work Manager	
Name:	Kirsty McArthur
Contact Telephone No.:	03000 512657
Contact Address:	Benton Park View, Newcastle upon Tyne NE98 1YX
email:	kirsty.mcarthur@hmrc.gov.uk
HMRC Authorised Officer: (Sponsor/Budget Approver/Invoicing & timesheets)	Bal Moore

A2.	**Supplier Information**
Supplier:	Gartner UK Limited
Contact:	Andrew Murray
Contact Tel No:	07507672393
Contact Address:	Tamesis, The Glanty, Egham, Surrey, TW20 9AH
email:	andrew.murray2@Gartner.com

A3.	**Contractual Detail**
Special Terms and Conditions: e.g. overtime, expenses, travel & subsistence, notice period.	This agreement will be governed by HMRC's Mandatory Clauses as set out within Appendix 1: Authority's Mandatory Terms in addition to the Supplier's General Terms included in Appendix 2. As this agreement is being issued under the Terms & Conditions of a non-HMRC contract, the following HMRC specific Terms & Conditions will also apply: I. The Contractor shall at all times comply with the Value Added Tax Act 1994 and all other statutes relating to direct or indirect tax. II. Failure to comply may constitute a material breach of this Contract and

	the Client may exercise the rights and provisions conferred by the Condition of Termination in the relevant contract. III. The Contractor shall furnish to the Client the name, and if applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or Self-Assessment reference of any agent, supplier or sub- contractor. Upon a request by the Client, the Contractor shall not employ or will cease to employ any agent, supplier of sub-contractor. By entering into this agreement, the Client will deem that the Contractor accepts the above HMRC specific Terms and Conditions.

A4.	Project Information
Project Title	CSG - Expert Insight and advisory support
Primary Location: (including full address)	Remote
Services Start Date:	1st January 2023
End Date:	31st December 2023

A5. Commercial Detail

Service Name	Level of Access	Quantity	Name of User to be Licensed	Contract Term Start Date	Contract Term End Date	Total Fee GBP
Gartner for Customer Service and Support Leaders Team	Team Leader	1	Bal Moore	01-JAN-2023	31-DEC-2023	£22,700
Gartner for Customer Service and Support Leaders Team	Advisor Team Member	1	TBC	01-JAN-2023	31-DEC-2023	£22,700
				Term Total	**(Excluding applicable taxes)**	**£45,400**

Grand Total (£) exclusive of VAT:	45,400

A6. Specification

The section below should be used to provide clear details relating to the requirements for delivery of the project/assignment. It should include, where appropriate, milestones / key deliverables with dates, and proposals for skills transfer.

The Contractor will deliver the requirement according to the provisions set out under A.5 Commercial Detail and section 2. Service Descriptions within Appendix 2: Gartner UK Limited Service Agreement for HM Revenue and Customs ("Client") of this agreement.

The Agreement effected by the signing of this Form of Agreement constitutes the entire agreement between the Parties relating to the subject matter of the Agreement and supersedes all prior negotiations, representations or understandings whether written or oral.

Signed for and on behalf of:

	The Commissioners for HM Revenue & Customs:		**Gartner UK Limited**
Signature:	DocuSigned by: Nicola Wenham CE66F4F01ED646C...	Signature:	DocuSigned by: Harry Capjon 4A5AAC184DD3405...
Name:	Nicola Wenham	Name:	Harry Capjon
Capacity:	Principle Sourcing Lead	Capacity:	Manager
Date:	22 December 2022	Date:	23 December 2022
Address:	Floor 1, Trinity Bridge House, 2 Dearmans Place, Salford, M3 5BS	Address:	Gartner UK Limited, Tamesis, The Glanty, Egham, Surrey TW20 9AW, United Kingdom
Telephone:	03000 536234	Telephone:	07892759098
email:	nicola.wenham@hmrc.gov.uk	email:	harry.capjon@gartner.com

Appendix 1
AUTHORITY'S MANDATORY TERMS

A. For the avoidance of doubt, references to 'the Agreement' mean the attached Service Agreement included in Appendix 2 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 Appendix 1.

C. In case of any ambiguity or conflict, the Authority's mandatory terms in this Appendix 1 will supersede any other terms in the Agreement.

D. For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority's mandatory terms in this Appendix 1 are the definitions set out at Clause 1 of this Appendix 1.

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 Service Order Form;
"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 UK GDPR;
"Data Protection Legislation"	a. "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and; b. all applicable Law about the processing of personal data and privacy;
"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 Service Agreement;

"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 UK 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;
"UK GDPR"	the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"VAT"	value added tax as provided for in the Value Added Tax Act 1994.

2. **Payment and Recovery of Sums Due**

1. The Supplier shall invoice the Authority as specified in Clause 3 of the Service 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:
    1. the Supplier does so at its own risk; and
    2. the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.
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.
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**

1. The Supplier represents and warrants that:
    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;
    2. it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and
    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.
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. 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 Service Agreement 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**

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

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

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.

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.

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.

7. If the Supplier:

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;

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

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).

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**

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.

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.

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.

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).

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:

1. Fraudulent evasion[2];
2. Conduct caught by the General Anti-Abuse Rule[3];
3. Conduct caught by the Halifax Abuse principle[4];
4. Entered into arrangements caught by a DOTAS or VADR scheme[5];
5. 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;
6. Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];

7. 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:

1. 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.
2. 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.
3. 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.
4. In respect of (f) this condition is satisfied without any further steps being taken.
5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

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.

Appendix: 2:

Gartner UK Limited Service Agreement for HM Revenue and Customs ("Client")

This Service Agreement ("**SA**"), including the General Terms and all applicable Service Descriptions, constitutes the complete agreement between **Gartner UK Limited** of Tamesis, The Glanty, Egham, Surrey, TW20 9AH ("**Gartner**") on behalf of itself and all wholly-owned affiliates of Gartner, Inc. and Client of 100 Parliament Street, Westminster, London, SW1A 2BQ for the Services (as defined below), and shall be effective when signed by both parties. Client agrees to subscribe to the following Services for the term and fees set forth below.

1. DEFINITIONS AND ORDER SCHEDULE

Services are the subscription-based research and related services purchased by Client in the Order Schedule below and described in the Service Descriptions. Service Names and Levels of Access are defined in the Service Descriptions. Gartner may periodically update the names and the deliverables for each Service. If Client adds Services or upgrades the level of service or access, an additional Service Agreement will be required.

Service Descriptions describe each Service purchased, specify the deliverables for each Service, and set forth any additional terms unique to a specific Service. Service Descriptions for the Services purchased in this SA may be viewed and downloaded through the hyperlinks listed in Section 2 below or may be attached to this SA in hard copy, and are incorporated by reference into this SA.

Service Name	Level of Access	Quantity	Name of User to be Licensed	Contract Term Start Date	Contract Term End Date	Total Fee GBP
Gartner for Customer Service and Support Leaders Team	Team Leader	1	Bal Moore	01-JAN-2023	31-DEC-202	£22,700
Gartner for Customer Service and Support Leaders Team	Advisor Team Member	1	TBC	01-JAN-2023	31-DEC-2023	£22,700
				Term Total	**(Excluding applicable taxes)**	**£45,400**
					Grand Total (£) exclusive of VAT:	45,400

1-2BXA96KR 2310 WRD

2. SERVICE DESCRIPTIONS

Service Name/ Level of Access	**Service Description URL**
Customer Service & Support Leaders Team: Team Leader	__https://sd.gartner.com/sd_css_team_leader.pdf
Customer Service & Support Leaders Team: Advisor Team Member	https://sd.gartner.com/sd_css_team_advisor_member.pdf

3. PAYMENT TERMS

Gartner will invoice Client annually in advance for all Services. Client agrees to pay any sales, use, value-added, or other tax or charge imposed or assessed by any governmental entity upon the sale, use or receipt of Services, with the exception of any taxes imposed on the net income of Gartner. Client agrees to pay all invoiced amounts within 30 days from the date of invoice.

4. CLIENT BILLING INFORMATION

Please attach any required Purchase Order ("**PO**") to this SA and enter the PO number below. If an annual PO is required for multi-year contracts, Client will issue the new PO at least 30 days prior to the beginning of each subsequent contract year. Any pre-printed or additional contract terms included on the PO shall be inapplicable and of no force or effect.

Purchase Order Number	*Billing Address*
VAT Number	*Invoice Recipient Name*
Invoice Recipient Tel. No.	*Invoice Recipient Email*

5. AUTHORISATION

Client: **HM Revenue and Customs**	**Gartner UK Limited**
Signature	*Signature*
Date	*Date*
Print Name	*Print Name*
Title	*Title*

IF NOT USING DIGITAL SIGNATURE, PLEASE RETURN TWO SIGNED ORIGINAL HARDCOPIES OF THIS SA TO:

Contracts Administration Department
Gartner UK Limited
Tamesis, The Glanty
Egham, Surrey
TW20 9AH

General Terms

1. This SA for subscription-based research and related services (the "Services") is non-cancellable, and may be terminated only for material breach by either party, upon 30 days prior written notice, if the breach is not cured within the notice period.

2. *Ownership and Use of the Services*. Gartner owns and retains all rights to the Services not expressly granted to Client. Only the individuals named in this SA (each a "**Licensed User**") may access the Services. Each Licensed User will be issued a unique password, which may not be shared. Client agrees to review and comply with the *Gartner Usage Policy* which is accessible to all Licensed Users via the "Policies" section of gartner.com. Among other things, the *Gartner Usage Policy* describes how Client may substitute Licensed Users, excerpt from and/or share Gartner research documents within the Client organization, and quote or excerpt from the Services externally.

3. *Client Confidential Information.* Gartner agrees to keep confidential any Client-specific information communicated by Client to Gartner in connection with this SA that is (i) clearly marked confidential if provided in written form, or (ii) preceded by a statement that such information is confidential, if provided in oral form, and such statement is confirmed in writing within 15 days of its initial disclosure. This obligation of confidence shall not apply to any information that: (1) is in the public domain at the time of its communication; (2) is independently developed by Gartner; (3) entered the public domain through no fault of Gartner subsequent to Client's communication to Gartner; (4) is in Gartner's possession free of any obligation of confidence at the time of Client's communication to Gartner; or (5) is communicated by the Client to a third party free of any obligation of confidence. Additionally, Gartner may disclose such information to the extent required by legal process.

4. *Disclaimer of All Other Warranties*. The Services are provided on an "as is" basis, and Gartner expressly disclaims all warranties, express or implied, statutory or otherwise, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, and warranties as to accuracy, completeness or adequacy of information. Client recognises the uncertainties inherent in any analysis or information that may be provided as part of the Services, and acknowledges that the Services are not a substitute for its own independent evaluation and analysis and should not be considered a recommendation to pursue any course of action. Gartner shall not be liable for any actions or decisions that Client may take based on the Services or any information or data contained therein. Client understands that it assumes the entire risk with respect to the use of the Services.

5. *Data Protection*. In performing its obligations under this SA, Gartner and the Client will each comply with the United Kingdom Data Protection Act 2018, any subordinate legislation passed under that Act and with any other applicable data protection legislation. In providing the services Gartner shall comply with its global privacy policy available at gartner.com/privacy.

6. *Miscellaneous*

(a) ***Assignability.*** This SA and the rights granted to Client hereunder may not be assigned, sublicensed or transferred, in whole or in part, by either party without the prior written consent of the other party, except to a successor to substantially all of the business or assets of a party by merger or acquisition. Where consent is required, it will not be unreasonably withheld.

(b) ***Dispute Resolution.*** Any unresolved dispute arising under this SA, including any question regarding its existence, validity or termination, shall at the request of either party, be referred to and finally resolved by arbitration under the London Chamber of International Arbitration ("LCIA") Rules. The number of arbitrators shall be one, to be agreed upon by the parties. If they are unable to so agree within 14 days of the date of the request that the dispute be referred to arbitration, the arbitrator shall be selected and appointed by the LCIA Court. The arbitration shall be conducted in London, England in the English language. The parties agree that the decision of the arbitrator shall be final and binding. This section is without prejudice to either party's right to seek interim relief against the other party (such as an injunction) through the English courts to protect its rights and interests. The prevailing party in any arbitration shall be entitled to an award of its reasonable attorneys' fees and costs, in addition to any award of damages or other relief.

(c) ***Applicable La***w. This SA shall be governed by and construed in accordance with the laws of England.

(d) ***Use of Name, Trademark, and Logo***. Absent the prior written consent of the other party, neither party shall use the name, trademarks, or logo of the other in promotional materials, publicity releases, advertising, or any other similar publications or communications.

(e) ***No Third Party Beneficiaries***. This SA is for the benefit of the parties only.

(f) ***Surviving Clauses***. Sections 3, 4, 5, and 6 (b), (c), (d), (e) and (f) shall survive the termination of this SA.

Gartner

SERVICE DESCRIPTION
Attachment to the Service Agreement

GARTNER FOR CUSTOMER SERVICE & SUPPORT LEADERS TEAM: TEAM LEADER

Gartner for Customer Service & Support Leaders: Team Leader (the "Service") is designed for senior customer service and support leaders, typically the head of customer service and support, and their leadership team. The Service provides client ("Client") with (i) an ongoing advisory relationship with research experts, and (ii) access to research covering the customer service and support sector and specific customer service and support roles in a team environment. The Service requires the separate purchase of Gartner for Customer Service & Support Leaders Team Member Services.

DELIVERABLES

The Gartner for Customer Service & Support Leaders Team is comprised of two sets of users: (i) the "Team Leader", and (ii) those "Team Members" designated by Client and listed in the Service Agreement. Collectively, the Team Leader and select Team Members are "Licensed Users".

1. The Deliverables for the Team Leader are set forth below.

- Gartner Research for Customer Service and Support Roles
- Peer & Practitioner Research
- Tools and Templates
- Functional Diagnostics
  Peer Benchmarks and Case Studies
- Individual Inquiry
- Team Inquiry
- Peer Networking
- Peer Meetings
- Webinars

- Additional information on the Deliverables listed above include the following:
  - Licensed Users may deploy Functional Diagnostics to both Licensed and Non-Licensed Users within the client company. Team Leader may deploy each survey product only once in each 12-month (twelve-month) period.
  - Team Leader may forward to others in the client company up to 25 (twenty-five) Gartner Research documents per contract year. This forwarding may not be done in a manner that has the intent or effect of avoiding the purchase of additional User licenses.

***

ADDITIONAL USAGE INFORMATION

Participation in inquiry calls is limited to the Licensed User(s) and Research Expert ("expert") only (i.e., non-Users, either inside or outside the client company, may not attend or otherwise participate on an inquiry call). The Team Leader is entitled to two types of inquiry: (i) inquiry sessions with an expert ("Individual Inquiry") which may be scheduled independent of other Team Members; and (ii) inquiry sessions with an expert and other members of the Customer Service & Support Leaders Team ("Team Inquiry"). For Team Inquiry sessions: (i) the Team Leader must schedule and attend the sessions; and (ii) Team Members may lead the discussion or pose questions to the expert on behalf of the team, provided all such questions and discussions advance the Team Leader's agenda.

Client companies around the world trust Gartner to be objective and independent in its research and advice, and Gartner takes that responsibility seriously. To preserve the objectivity of research, Gartner does not promise Clients favorable coverage or leads from its research experts. Gartner does not provide access to

confidential client information, offer aid to secure capital funding, or sell any product for use in litigation. There are no exceptions. If you have questions, please email ombuds@gartner.com.

Use of this Service is governed by the Gartner Usage Policy and the Gartner Content Compliance Policy which are accessible on the Policies section of gartner.com.

SERVICE DESCRIPTION
Attachment to the Service Agreement

GARTNER FOR CUSTOMER SERVICE & SUPPORT LEADERS TEAM: ADVISOR TEAM MEMBER

Gartner for Customer Service & Support Leaders Team: Advisor Team Member (the "Service") is designed for senior customer service and support leaders. The Service provides client ("Client") with (i) an ongoing advisory relationship with research experts, and (ii) access to research covering the customer service and support sector and specific customer service and support roles in a team environment. This Service requires the separate purchase of a Customer Service & Support Leaders Team Leader Service.

DELIVERABLES

Gartner for Customer Service & Support Leaders Team is comprised of two sets of users: (i) the "Team Leader", and (ii) those team "Team Members" designated by Client and listed in the Service Agreement. Collectively, the Team Leader and select Team Members are "Licensed Users".

1. The Deliverables for the Advisor Team Member are set forth below.

- Gartner Research for Customer Service and Support Roles
- Peer & Practitioner Research
- Tools and Templates
- Functional Diagnostics
  Peer Benchmarks and Case Studies
- Individual Inquiry
- Team Inquiry
- Peer Networking
- Peer Meetings
- Webinars

- Additional information on the Deliverables listed above include the following:
  Licensed Users may deploy Functional Diagnostics to both Licensed and Non-licensed Users in the client company.

***

ADDITIONAL USAGE INFORMATION

Participation in inquiry calls is limited to Licensed User(s) and Research Expert ("expert") only (i.e., non-Users, either inside or outside of the client company, may not attend or otherwise participate on an inquiry call). Team Members are entitled to two types of inquiry: (i) inquiry sessions with an expert ("Individual Inquiry") which may be scheduled independent of other Team Members; and (ii) inquiry sessions with an expert and the Customer Service & Support Leaders Team ("Team Inquiry"). For Team Inquiry sessions:

- the Team Leader must schedule and attend the sessions; and (ii) Team Members may lead the discussion or pose questions to the expert on behalf of the team, provided all such questions and discussions advance the Team Leader's agenda.

Client companies around the world trust Gartner to be objective and independent in its research and advice, and Gartner takes that responsibility seriously. To preserve the objectivity of research, Gartner does not promise Clients favorable coverage or leads from its research experts. Gartner does not provide access to confidential client information, offer aid to secure capital funding, or sell any product for use in litigation. There are no exceptions. If you have questions, please email ombuds@gartner.com.

Use of this Service is governed by the Gartner Usage Policy and the Gartner Content Compliance Policy which are accessible on the Policies section of gartner.com.

Appendix C: Security Questionnaire Plan

HM Revenue & Customs

Security Plan Questionnaire - Low

To:	**Gartner UK Limited**
From:	**Fintan Bradley**
Date:	**07 December 2022**
Tender reference:	**CSG – Expert Insight and Advisory Support**
Tender title:	**SR1201952481**

Schedule 2.4 Security Plan

Background
The Contractor is required to prepare a Security Plan in accordance with the 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. **The content of the contract will be subject to negotiation. We confirm our understanding that our answers to the security questionnaire will form the initial security plan.**
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. **n/a**
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 sub-contractors, please provide details of how you will conform to this. **We do not believe this is applicable**
1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK GDPR and in accordance with Clause 23 (*Protection of Personal Data*) of the Contract. **Gartner operates as a data controller in compliance with applicable laws, including UK data protection law.**
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 **Confirmed**
1f Please provide details of any security accreditation that your organisation currently possesses, such as but not exclusive to, ISO27001 and PCI DSS and describe the process used for achieving the accreditation. **Attached ISO 27001 certificate**
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. **n/a**
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. **Our data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems. In order to detect the presence of water leaks, the data centers have functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.**
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 building construction type, 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. **Gartner's data center providers utilize physical security boundaries and entry controls to prevent unauthorized physical access, damage and interference to information processing facilities hosting Gartner data.**
3 IT Security (For requirements please see Appendix B – IT Security)
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. **We have Cyber Essential 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. **The entire network is subject to regular red team testing (e.g. breach and attack simulation) and at least annual external penetration testing. We leverage global security researcher talent via a private, continuous, crowdsourced reporting program, for detecting and reporting on vulnerabilities in Gartner enterprise and digital markets properties. The entire network utilizes a DLP solution that offers complete data protection with full context and content inspection for all data in motion, as well as advanced features, including Exact Data Match, machine learning, and granular policies for optimal protection. It is architected to sit inline, so it can block sensitive information before it leaves your network instead of being limited to damage control after data has been compromised. The Data is properly classified, labelled and protected and Gartner makes sure to monitor information systems in use which is processed for intrusions, loss and other unauthorized activity. Our DLP solution uses industry standard host, network, and cloud-based Intrusion Detection Systems (IDS) and has implementation of advanced Intrusion Protection Systems (IPS) configured to monitor and actively stop data loss. All intrusions are inspected and require an analysis of the system to ensure any residual vulnerabilities are also addressed.**

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. **Gartner has a formal Access Control process that includes role-based access control to computing platforms and applications. Unique users are created and disabled automatically based on the employee's status in our HR system. Access is controlled by creating dynamic groups and dynamic objects which automate the granting of permissions following the principle of least privilege. Access to elevated privileges and other special access requests is submitted through an additional access form. The request is then reviewed and processed.**
3d Please provide details of how your security and access control policy complies with Security Policy Framework requirements 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. **Multi Factor Authentication is required for any remote access that is off the Gartner network, including access to cloud or web applications. Remote access VPN and virtual office are segmented as DMZ networks hosted on firewall enclaves independent of server production networks. Remote Access VPN utilizes AES-256 bit encryption. Certificates are required for access.**
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). **The entire network is subject to regular red team testing (e.g. breach and attach simulation) and at least annual external penetration testing. We leverage global security researcher talent via a private, continuous, crowdsourced reporting program, for detecting and reporting on vulnerabilities in Gartner enterprise and digital markets properties.**
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. **Gartner's cloud environments, data at rest is encrypted by utilizing the native encryption services offered by the cloud provider. Where we have identified data that is very sensitive, additional symmetric or asymmetric encryption may be used on top of native encryption protocols. Gartner requires Full Disk Encryption on PCs. The task includes configuring computers/servers with Gartner-approved encryption software and approving encryption products and algorithms to mitigate the risk of data exposure. All Gartner entities utilizing and supporting cryptography ensure they comply with Gartner encryption standards.**
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. **For client confidential information, we delete the information upon client request.**
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). **Please see attached Gartner's Background Check Policy. We employ the principle of least privilege, and access is restricted to the minimum entitlements necessary for associates to perform their roles. Only the required staff will have access to the client data. Gartner completes the below:** **• Verify ID documentation (passport, right to work etc)** **• Use national ID numbers, such as SSNs in the US, to support the criminal check, where such numbers exist. (e.g. in the UK we complete BPSS checks)** **• Verify the most recent educational credentials (highest degree obtained), employment and criminal history for a period of 7 years in the US and 5 years outside of the US.** **• Provide for a consistent means of validating eligibility across locations (e.g., falsification of educational credentials will be a disqualifying result in all locations, within any local legal limits).** **• In some instances, based on the role, geography, or particular assignments, drug screening and credit checks may also be included.**
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? **All employees are required to adhere to the same internal Gartner standards, policies and procedures, and to complete appropriate training on an annual basis.**
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 (CA). Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the NDA for all personnel involved in this Contract if requested. **Confidentiality obligations should be maintained at a corporate level between entities. All employees have provided confidentiality commitments to Gartner as part of their employment agreement.**
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. **Data is logically segregated using a tenant identifier.**
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 including any associates/sub-contractors) is prohibited without prior written consent from the 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. **Gartner stores data in an AWS Datacenter – AWS US-East 1 (Northern Virginia) & US-East 2 (Ohio) - Hosting. There is not another third party involved in this service.**

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.

If you are considering transferring data outside of the UK, please provide details on how and where the data will be processed or stored.

To the extent that any data offshoring would include the transfer of Personal Data (as defined in the United Kingdom General Data Protection Regulation (UK GDPR)) outside of the UK, please provide details of the protections and safeguards which would be applied to ensure that such data is afforded a level of protection that is essentially equivalent to that guaranteed in the UK by UK GDPR, including in relation to access to the data by the country's public authorities.

Please note: In line with HMRC's current policies, the successful supplier(s) will not be permitted to transfer any Personal Data provided by HMRC in connection with any contract resulting from this procurement exercise to any country outside of the UK where such transferred data will not be afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR.

On this basis, HMRC reserves the right to reject a bidder's entire tender submission and/or terminate any contract awarded where it becomes apparent to HMRC that the supplier is transferring/is proposing to transfer Personal Data outside of the UK without ensuring the transferred data is afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR.

Gartner acts as a data controller, we do not operate as a data processor. Gartner will collect the personal data directly from the data subjects (the Licensed Users) during the registration process. It's Gartner alone who determines the means and purposes of such collection and handling of personal data. Our clients do not determine what personal data is necessary for Gartner to provide the services, and clients do not instruct Gartner how to use that personal data in the delivery of the contracted services.

Gartner is a global company and we may transfer personal information to other Gartner group companies or suppliers outside your country. Gartner will take reasonable steps to ensure that personal information is protected and any such transfers comply with applicable law.

Gartner may transfer and maintain the personal information of individuals covered by this Policy on servers or databases outside the European Economic Area ("EEA"). Some of these countries may not have the equivalent level of protection under their data protection laws as in the EEA. The countries to which we transfer data outside of the EEA may include any of the countries in which Gartner does business. A list of Gartner office locations can be found here: https://www.gartner.com/technology/contact/worldwide_offices.jsp.

All Gartner entities have signed an Intragroup Agreement containing the European Union ("EU") Commission Approved Standard Contractual Clauses for the transfer of data outside the European Economic Area. All Gartner entities have the same technical, physical,

SD2.4c OFFICIAL and administrative security controls and are required to comply with our data protection policies and procedures, applicable laws, and the terms of our client and member contracts governing the collection and use of information. **Gartner associates servicing the HMRC contract will ensure HMRC's data is not serviced by associates in our China office (Gartner no longer have a Russia office).**
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. **Gartner has a formal Access Control process that includes role-based access control to computing platforms and applications. Unique users are created and disabled automatically based on the employee's status in our HR system. Access is controlled by creating dynamic groups and dynamic objects which automate the granting of permissions following the principle of least privilege. Access to elevated privileges and other special access requests is submitted through an additional access form. The request is then reviewed and processed.**
5e What arrangements are in place for secure disposal of HMRC assets once no longer required? **As the desired data retention period varies widely among clients, we delete client data at the request of our clients or after the retention period specified in our agreement with the particular client. Accordingly, we ask that clients specify how long they would like us to retain data.** **We do not routinely delete personal data from our systems at the end of a client's contract term with us (or shortly thereafter). In most cases we have regulatory or statutory reasons to keep the personal data for longer than that. Exactly how long depends on what we collected the data for and other factors, but we here we are talking about years rather than months.** **An important point to note is that the Data Subject (i.e. the individual that the personal data relates to) has a number of rights which include requesting access, restricting use, request deletion and so forth. These rights are for the individuals rather than for the client company.** **As a company we collect only a very limited amount of personal data in connection with our services and it mainly consists of contact details.** **5. RETENTION PERIODS We will retain your personal information for as long as required to perform the purposes for which the data was collected, depending on the legal basis for which that data was obtained and/or whether additional legal/regulatory obligations require us to retain it.** **In general terms, this will mean that your personal information will be kept for the duration of our relationship with you and:** **• the period required by tax and company laws and regulations; and** **• as long as it is necessary for you to be able to bring a claim against us and for us to be able to defend ourselves against any legal claims. This will generally be the length of the relationship plus the length of any applicable statutory limitation period under local laws.**

5f How and when will you advise HMRC of security incidents that impact HMRC assets. **Gartner has a default client incident notification period of 72 hours. 72 hours provides Gartner's Incident Response Team a greater opportunity to identify, contain, and remediate an incident swiftly. Notification and reporting increase the administrative overhead of an incident and generally pull key resources away from the actionable phases of the incident response process.** **72 hours provides Gartner's Incident Response Team a greater opportunity to identify, contain, and remediate an incident swiftly. Notification and reporting increase the administrative overhead of an incident and generally pull key resources away from the actionable phases of the incident response process.** **72 hours is the right balance between giving Gartner a good sense of the situation, which makes the client's reporting easier and better as well while providing clients the information quickly at the same time.**
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 HMRC data under the Contract, or attach a copy of your Business Continuity Plan. **Attached ToC** **Gartner has established a consistent unified framework for business continuity planning and plan development, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. The business continuity plan includes the following:** **• Defined purpose and scope, aligned with relevant dependencies** **• Accessible to and understood by those who will use them** **• Owned by a named person who is responsible for their review, update, and approval** **• Defined lines of communication, roles, and responsibilities** **• Detailed recovery procedures, manual work-around, and reference information** **• Method for plan invocation**

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 - Preferably 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	Visitor 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 previously agreed processes with HMRC.	Point to point transfer 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 self-assessment 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[1]	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. Password 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.	

[1] 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).

IT Security	Requirements	Recommended
Malware Protection[2]	Controls such as anti-virus software must detect and prevent infection by known malicious code.[3] AV Administrators and users should be trained on use of AV software. Users should receive awareness training so that they are aware of risks posed by malicious code from the use of email and 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.	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.
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.

[2] 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.
[3] 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.

IT Security	Requirements	Recommended
Disposal of media	HMRC information assets must be sanitised in line with the Security Policy Framework.	
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[4]. 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 BPSS, available from ww.gov.uk, specifically the information relating to the Disclosure & Barring Service for more information.
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.

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

Appendix D – Process Security

Process Security	Requirements	Recommended
Security Policies, Processes and Procedures	Procedures should 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 HMRC's assets are segregated from any other Client's assets held by the contractor. Procedures for the secure disposal of 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.

Process Security	Requirements	Recommended
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 the 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 the 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	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	