Chartered Institute of Internal Auditors

Dated 19th June 2020

Chartered Institute of Internal Auditors

and

The Government Internal Audit Agency (GIAA)

External Quality Assessment (EQA) Agreement

THIS AGREEMENT is made on the 19th June 2020

BETWEEN:

(1) **Chartered Institute of Internal Auditors** whose registered office is at 13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX (the "Supplier"); and

(2) **The Government Internal Audit Agency (GIAA)** whose principal office is at 10 Victoria Street, London, SW1H 0NB (the "Buyer").

1. Definitions

"Buyer"	means The Government Internal Audit Agency
Controller"	has the meaning given to it in the GDPR;
"Data Protection Legislation"	means the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 ("GDPR");
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"Good Industry Practice"	standards, practices, methods and procedures conforming to the law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government 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, including any of the Buyer's confidential information, and which: i) are supplied to the Supplier by or on behalf of the

	Buyer; or ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or b) any Personal Data for which the Buyer is the Data Controller;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Processor"	has the meaning given to it in the GDPR;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of the Supplier related to the Contract;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"**Supplier**"	means the Chartered Institute of Internal Auditors
"the Services"	means the consultancy services set out in Schedule 1 and any such other services as shall be mutually agreed from time to time;

2. Obligations

2.1 The Supplier shall:

2.1.1 perform the Services with such skill and care as to be in accordance with best practice;

2.1.2 provide the Services in a timely and efficient manner and to the satisfaction of and in accordance with a timetable to be agreed between the parties;

2.1.3 provide the Services at the Buyer's premises or from other premises as directed by the Buyer;

2.1.4 keep records of all actions and undertaking carried out by the Supplier in relation to the provision of the Services and at the Buyer's request shall make them available for inspection and/or provide copies to the Buyer;

2.1.5 perform all duties contemplated by the Services or as agreed from time to time.

2.2 The Buyer and the Supplier acknowledge that this is a contract for services and not a contract of employment.

3. The Buyer's obligations

The Buyer shall:

3.1 afford to the reviewers, during the Buyer's normal business hours, such access to its premises, staff, information and records as the reviewers may reasonably require to provide the Services; and

3.2 provide information to the Supplier within a reasonable timeframe prior to the site visit so that the review team can be fully prepared; and

3.3 make available to the reviewers such working space and facilities on its premises as the reviewers may reasonably require for the performance of the Services, subject to above.

4. Disclosure / Use of Information

Both parties agree:

4.1 that they will not disclose to any third parties or elsewhere, nor copy or use in any way, nor cause to be used in any way, any confidential information other than:

(a) in the case of the Supplier, as authorised in writing by the Buyer and deemed essential for the duties contemplated by the Services; and

4.2 neither party shall use the other party's name, trademarks, service marks, logos, trade names and/or branding without such party's prior written consent.

For the purpose of this agreement, *confidential information* refers to all electronic, oral, written, graphic or information in any other form of a confidential nature including but not limited to any financial, technical, commercial information or data, business proposals, projects/proposals of any kind, information relating to ideas or inventions of both parties, designs or formulae, know how, intellectual property, database information, business forecasts and personnel matters.

5. Confidentiality

The Supplier shall, and shall ensure that the reviewers shall:

keep secret and confidential all the confidential information disclosed by the Buyer or otherwise coming into its or their knowledge in the course of, or for the purpose of, the provision of the Services, and undertake not to disclose the confidential information to any third party without the Buyer's prior written consent;

at any time on request by the Buyer, and in any event without request on expiry or termination (for whatever reason) of this agreement, promptly return all documents and material containing confidential information without keeping any copies.

The Supplier shall be liable to indemnify the Buyer, its officers, directors, employees and affiliates against any loss, liability, claim, damage, suit, proceeding and/or action brought against the Buyer by any third party or due to misuse of Confidential Information by the Supplier or any of its reviewers.

6. Assignment and Sub-contracting

This agreement is between the Buyer and the Supplier, who may not assign, transfer, subcontract or otherwise in any other manner make over the benefit and/or burden of this agreement to any third party without the express prior written consent of the Buyer.

7. Terms and Termination

7.1 This agreement commences on the date specified above and expires following the completion of the Services and payment of the fees.

7.2 Either party may terminate this agreement forthwith by written notice if the other party:

7.2.1 is in material breach of the terms of this agreement which, in the case of a breach capable of remedy, is not remedied within 7 days of receipt of notice specifying the breach and requiring its remedy.

7.3 Upon termination the Supplier must promptly delete or return the Government Data except where required to retain copies by law.

8. Fee

The agreed fee is set out in Schedule 1. For time critical and agreed timeframes, the Supplier reserves the right to amend the agreed fee if the Buyer requests additional work that was not in the original proposal. Any amendment of fee shall, at all times, be pre-agreed in writing with the Buyer.

9. Dispute

9.1 Governing Law

The parties hereto agree that this agreement is governed by English Law.

9.2 Jurisdiction

The courts of England shall have the jurisdiction to settle any dispute arising out of or in connection with this agreement but without prejudice to the Buyer's general right to issue proceedings, when necessary, in any court in any jurisdiction whatsoever.

10. Data protection

10.1 The Buyer is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation.

10.2 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with this Contract.

10.3 The Supplier must not remove any ownership or security notices in or relating to the Government Data. For the purposes of the Contract the supplier will ONLY access documents marked OFFICIAL and will comply with any relevant provisions of GIAA's security policy relating to security of these documents as directed by the GIAA project leads

10.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified [in writing] by the Buyer.

10.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under the Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Buyer and immediately suggest remedial action.

10.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
(a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than five Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier;
(b) restore the Government Data itself or using a third party.

10.7 The Supplier must pay each Party's reasonable costs of complying with clause 10.6 unless the Buyer is at fault.

10.8 Only the Buyer can decide what processing of Personal Data a Supplier can do under the Contract and must specify it for the Contract using the template in Annex 1 (*Authorised Processing*).

10.9 The Supplier must only process Personal Data if authorised to do so in the Annex 1 (*Authorised Processing*) by the Buyer. Any further written instructions relating to the processing of Personal Data are incorporated into Annex 1.

10.10 The Supplier must give all reasonable assistance to the Buyer in the preparation of any Data Protection Impact Assessment before starting any processing, including:
(a) a systematic description of the expected processing and its purpose;
(b) the necessity and proportionality of the processing operations;
(c) the risks to the rights and freedoms of Data Subjects;
(d) the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.

10.11 The Supplier must notify the Buyer immediately if it thinks the Buyer's instructions breach the Data Protection Legislation.

10.12 The Supplier must put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Buyer.

10.13 If lawful to notify the Buyer, the Supplier must notify it if the Supplier is required to process Personal Data by Law promptly and before processing it.

10.14 The Supplier must take all reasonable steps to ensure the reliability and integrity of any Supplier Staff who have access to the Personal Data and ensure that they:
(a) are aware of and comply with the Supplier's duties under this clause 7;
(b) are subject to appropriate confidentiality undertakings with the Supplier or any Subprocessor;
(c) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third Party unless directed in writing to do so by the Buyer or as otherwise allowed by the Contract;
(d) have undergone adequate training in the use, care, protection and handling of Personal Data.

10.15 The Supplier must not transfer Personal Data outside of the EU unless all of the following are true:
(a) it has obtained prior written consent of the Buyer;

(b) the Buyer has decided that there are appropriate safeguards (in accordance with Article 46 of the GDPR);
(c) the Data Subject has enforceable rights and effective legal remedies when transferred;
(d) the Supplier meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;
(e) where the Supplier is not bound by Data Protection Legislation it must use its best endeavours to help the Buyer meet its own obligations under Data Protection Legislation; and
(f) the Supplier complies with the Buyer's reasonable prior instructions about the processing of the Personal Data.

10.16 The Supplier must notify the Buyer immediately if it:
(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; (f) becomes aware of a Data Loss Event.

10.17 Any requirement to notify under clause 10.16 includes the provision of further information to the Buyer in stages as details become available.

10.18 The Supplier must promptly provide the Buyer with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 10.16. This includes giving the Buyer:
(a) full details and copies of the complaint, communication or request;
(b) reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
(c) any Personal Data it holds in relation to a Data Subject on request;
(d) assistance that it requests following any Data Loss Event;
(e) assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office.

10.19 The Supplier must maintain full, accurate records and information to show it complies with this clause 10. This requirement does not apply where the Supplier employs fewer than 250 staff, unless either the Buyer determines that the processing:
(a) is not occasional;
(b) includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR;
(c) is likely to result in a risk to the rights and freedoms of Data Subjects.

10.20 The Supplier must appoint a Data Protection Officer responsible for observing its obligations in this Schedule and give the Buyer their contact details.

10.21 Before allowing any Subprocessor to process any Personal Data, the Supplier must:
(a) notify the Buyer in writing of the intended Subprocessor and processing;
(b) obtain the written consent of the Buyer;

(c) enter into a written contract with the Subprocessor so that this clause 10 applies to the Subprocessor;
(d) provide the Buyer with any information about the Subprocessor that the Buyer reasonably requires.

10.22 The Supplier remains fully liable for all acts or omissions of any Subprocessor.

10.23 At any time the Buyer can, with 30 Working Days notice to the Supplier, change this clause 10 to:
(a) replace it with any applicable standard clauses (between the controller and processor) or similar terms forming part of an applicable certification scheme under GDPR Article 42;
(b) ensure it complies with guidance issued by the Information Commissioner's Office.

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

10.25 The Supplier:
(a) must provide the Buyer with all Government Data in an agreed open format within 10 Working Days of a written request;
(b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
(c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
(d) securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it;
(e) indemnifies the Buyer against any and all Losses incurred if the Supplier breaches clause 10 and any Data Protection Legislation.

11. Entire Agreement

This agreement shall constitute the entire understanding between the parties in relation to the Services and shall supersede all prior agreements, negotiations and discussions between the parties in respect thereof.

12. Payment

Provided the Supplier has completed the Services in accordance with this Agreement, payment will be made by the Buyer within 30 days of receiving of an undisputed invoice from the Supplier. Payment shall be made in 2 parts at the conclusion of Phase 1 and Phase 2.

13. Work to be performed

The Supplier undertakes that the work to be performed will adhere to the terms specified in the official proposal “An Internal Audit External Quality Assessment for the Government Internal Audit Agency” submitted by the Supplier to the Buyer on the 29th April 2020.

14. Insurance

The Supplier has professional indemnity cover up to £5m and a copy of the insurance document can be provided upon request.

15. Notices

Unless otherwise specified, any communication to be made under or in connection with this agreement shall be made in writing and may be made by email or letter. The email and postal address (and contact name for whose attention the communication is made) of each party is:

For the Supplier:

Name: **REDACTED**
Job Title: **REDACTED**
Address: 13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX
Telephone No: **REDACTED**
Email address: **REDACTED**

For the Buyer: **REDACTED**
Name: **REDACTED**
Address: 10 Victoria Street, London, SW1H 0NB
Telephone No: **REDACTED**
Email address: **REDACTED**

SIGNED by

REDACTED

for and on behalf of the
CHARTERED INSTITUTE OF INTERNAL AUDITORS

SIGNED by

REDACTED

On behalf of
The Government Internal Audit Agency

Annex 1 – Authorised Processing

Contract:	**GIAA20A05.IIA.**
Date:	**22/06/2020**
Description Of Authorised Processing	**Details**
Subject matter of the processing	Internal audit files, processes and procedures.
Duration of the processing	June 2020 until approximately March 2021
Nature and purposes of the processing	For the EQA review team to review the level of performance of The GIAA team.
Type of Personal Data	Names and job roles Email addresses PMRs
Categories of Data Subject	GIAA Internal employees

SCHEDULE 1

SERVICES AND FEES

Services

The Supplier will provide a review team (nominated below) to carry out an External Quality Assessment (EQA) at the Buyer's premises with a technical review to be performed by the Supplier:

REDACTED

Supported remotely and quality assured by **REDACTED**, **REDACTED**

All our reviewers are experienced heads of internal audit, have passed the Chartered IIA's stringent assessment process and are members of the Chartered IIA, thereby ensuring they abide by our Code of Professional Conduct.

The Supplier will provide a draft report based on the findings at the conclusion of Phase 2.

Fees

The agreed fee payable to the Supplier for the performance of the Services in accordance with this Agreement is:

Fee: £106,500 exclusive of all reasonable expenses and VAT at 20%.

To be paid in 2 parts:

£63,900 exclusive of all reasonable expenses and VAT at 20% at the conclusion of phase 1.

£42,600 exclusive of all reasonable expenses and VAT at 20% upon issue of the draft report.