FORM OF CONTRACT

This contract is made on the 29th day of. September 2022

BETWEEN

(1) HM Revenue & Customs 100 Parliament Street, Westminster, London SW1A 2BQ , (the **"Customer"**); and

(2) Penna plc whose registered office is 10 Bishops Square, London, E1 6EG whose company number is 1918150 (the **"Service Provider"**)

WHEREAS the Customer wishes to have provided the following goods and/or services namely Strategic HR Services pursuant to the ESPO Framework Agreement (reference 3S-22).

NOW IT IS AGREED THAT

1. The Service Provider will provide the goods and/or services in accordance with the terms of the call-off contract (reference number 3S-22) and Contract Documents.
2. The Customer will pay the Service Provider the amount due in accordance with the terms of the call off agreement and the Contract Documents.
3. The following documents comprise the Contract Documents and shall be deemed to form and be read and construed as part of this agreement:
   - This Form of Contract
   - The Master Contract Schedule
   - The documents as
   - Security Questionnaire
   - **IN WITNESS OF** the hands of the Parties or their duly authorised representatives:

Signed for and on behalf of

HM REVENUE & CUSTOMS

by [redacted], an authorised officer

)

)

Authorised Officer

Print name:

Signed by

PENNA plc)

)

)

Service Provider

Print name:

EXECUTED AS A DEED BY THE CUSTOMER

by affixing the common seal of

[INSERT NAME OF CUSTOMER]

in the presence of :-

Authorised Officer

EXECUTED AS A DEED BY THE SERVICE PROVIDER

by affixing the common seal of

[INSERT NAME OF SERVICE PROVIDER]

in the presence of: -

.....

Director

.....

[Director **OR** Secretary]

OR

EXECUTED AS A DEED BY

[INSERT SERVICE PROVIDER'S NAME] **acting by**

[INSERT NAME OF FIRST DIRECTOR]**, a director and**

[INSERT NAME OF SECOND DIRECTOR/SECRETARY],

[a director OR its secretary]

.....

Director

….....

[Director **OR** Secretary]

This document relates to and forms part of the Call-Off Terms

(Document Reference SR 982744217)

MASTER CONTRACT SCHEDULE

(ESPO Framework Reference 3S-22 Strategic HR Services)

1. TERM

Commencement Date

23 September 2022

Expiry Date

22 September 2024

Extension Period

N/A

2. SERVICES REQUIREMENTS

Services and Deliverables required

INTRODUCTION

HM Revenue & Customs (HMRC) the Authority, are the UK's tax, payments and customs authority. Our purpose is to:

collect the money that pays for the UK's public services; and

help families and individuals with targeted financial support.

We do this by being impartial and increasingly effective and efficient in our administration. We help the honest majority to get their tax right and make it hard for the dishonest minority to cheat the system.

BACKGROUND

This is an annual recruitment for the Tax Specialist Tax Specialist Programme, a three year Tax Specialist Programme leading to Grade 7, being the primary supply chain for G7 tax professionals.

Initial recruitment is for around 200 trainees although for 2022 the number recruited is nearer 285 and is likely to be a similar number for 2023. The posts are located across all 13 regional locations.

The recruitment process is delivered via civil service jobs and has 3 stages. Stage 1 is on -line tests, stage 2 is video interviews and stage 3 is an assessment centre. The assessment centre is the final stage of selection.

CONTRACT SCOPE

The Supplier will be required to design and create three new assessment exercises and provide associated materials and support for HMRC's TSP Assessment Centre.

DETAILED REQUIREMENTS

HMRC TSP Virtual Assessment Centre Exercise Outline

Outline format of the assessment centre

- A half-day Centre with the following three 45-60 minutes exercises
  - Group discussion
  - Analysis exercise
  - Stakeholder engagement
- Designed to measure performance/potential across five behavioural areas in the Civil Service Success Profile Framework:
  - Working Together
  - Communication and Influencing
  - Delivering at Pace
  - Making Effective Decisions
  - Managing a Quality Service
- Exercises should have Thought Leadership principles designed in that are reflected in the behavioural indicators in the marking guides.
- Each competency should be measured at least twice in the centre.

Behavioural indicators to be assessed by each exercise

This matrix below indicates how behavioural indicators could be measured in the three exercises based on previous experience.

	Group Discussion	Stakeholder Engagement	Analysis Exercise
Working Together	**Y**	**Y**	
Communication and influencing	**Y**	**Y**	**Y**
Delivering at Pace	**Y**	**Y**	**Y**
Making Effective Decisions		**Y**	**Y**
Managing a Quality Service	**Y**		**Y**

Exercise Outlines

Ideally a fictitious scenario narrative should flow through all three exercises, although candidates will be provided with specific new information so that performance on each exercise will be independent from the others. but the scenario should mirror the ways of working of a governmental department to offer candidates a credible context; this is important for candidate engagement and will provide a fair opportunity for all candidates.

Exercise	Task and Proposed scenario	Approximate timing
Analysis Exercise	A two-option scenario where the candidate is tasked to carry out a balanced evaluation and recommend one option with rationale to be taken to a decision-making funding committee for agreement. Each option should have a number of wide-ranging commercial and social implications. Candidates should be provided with information in a range of formats, outlining each project's contribution to meeting key government targets in this area. Candidates will be asked to prepare a written summary of their analysis of the initiatives and recommendation (criteria to be decided). A Q&A session with an assessor (playing themselves) will follow, to explore their approach and understanding of the key issues in the brief.	• 40 minutes review and report writing • 10 minute break while assessor reads report • 15 minutes Q&A with an assessor to clarify decision
Group Exercise	The discussion will be based on six proposals each of which is a possible means of addressing/fulfilling a strategic objective of the fictitious government department. Each candidate will be provided with a brief consisting of an email from the departmental sponsor, a short summary of the six proposals, their individual more detailed summary of one of the proposals and a key to any tabulated information. Candidates will be tasked to come to agreement and provide a suitable briefing. They will be responsible for sharing the detail they have on their allotted option with others with obvious decisions around how positively and completely they divulge material information, and how collaborative they are when helping the group to reach a decision. As a group, they need to discuss the options and arrive at their preferences, in priority order.	• 15 minutes individual reading (extended by 5 minutes for groups of 5 or 4) • 40 minutes for the group meeting.

Stakeholder Briefing	The suggested scenario is a junior Project Manager helping a Senior Project Manager (assessor) to urgently review a project ahead of a key meeting later that day. The options will be to press ahead, scale down or postpone. The brief will set out the scenario and provide information from different sources that could impact on the decision. The candidate will have up to 25 minutes to read the information in the brief and prepare for their meeting with the assessor. There will be reasons for and against all options, and so what is important, is to understand how the candidate has made their decision. When the candidate has given their presentation, the assessor will have a number of core questions they need to ask them, to help the Senior Project Manager understand the key issues before the meeting. After asking the four core questions, they will select a group of specific questions which have been designed to have particular relevance to the recommendation made by the candidate. They will introduce some new piece of information.	• 25 minutes review of content • 5 minute verbal briefing • 20 minutes scripted Q&A challenge session

Additional information

You will need to provide or contribute to candidate pre-information on the Centre. This may include background scenario information on the fictitious department. This would not require any pre-centre submissions but will help orientate the candidate to the exercises and scenario.

DETAILED ASSESSMENT DESIGN AND MOBILISATION

The supplier must develop detailed assessment plans, to support the design and mobilisation of the Tax Specialist Programme as required within this specification. The supplier will:

- Provide a named, senior responsible owner for Tax Specialist Programme design, mobilisation and delivery work. This person must possess the management expertise required to oversee the assessment design exercises and provide advice and guidance to the customer.

- Lead the development of a detailed implementation plan covering all aspects of assessment design and delivery. A robust, detailed implementation plan must be in place within two

weeks of contract signature. Once developed the supplier will maintain and co-ordinate activity against this plan.

- Reflects the requirements of the Civil Service Success Profiles in fulfilling the 'behaviours' requirements in the standard (see Success Profiles - Civil Service Behaviours (publishing.service.gov.uk)); and

- Will be mobilised to deliver against the agreed implementation plan – including to the headline timescales defined in these tender documents, i.e ;

  Engage with Customer to launch the Tax Specialist Programme in September 2022.

  Re work if required and final sign off by Customer by end of November 2022

  Commence assessor training by end of November 2022.

Assessment Exercises

High-quality, engaging and flexible assessment exercises should be the core of the Tax Specialist Programme. The expectations of the supplier in relation to this aspect of the Tax Specialist Programme are therefore particularly high.

Requirements for delivery of training for new TSP Assessors.

The final stage of the Tax Specialist Tax Specialist Programme is an assessment centre and the assessors who participate will have undertaken training to be an effective assessor.

Each year we refresh the assessor pool and we want to run 2 training events for up to 30 new assessors. Each event will be 1 day and will accommodate up to 15 delegates. The training will be delivered face to face and take place in HMRC offices in Nottingham.

The training will cover the following:

An understanding of the Tax Specialist Tax Specialist Programme recruitment process.

The principles of robust and objective assessment using the ORCE model:

Observe

Record

Classify

Evaluate

Recognise the importance of keeping decision making objective and maintaining diversity in the talent pipeline

Build familiarity with the 3 new exercises.

Group Discussion

Analysis Exercise

Stakeholder Engagement.

TAX SPECIALIST PROGRAMME MANAGEMENT AND ADMINISTRATION

The supplier must have proven ability to effectively manage and administer the design and training of the recruitment assessment services. The supplier will:

- Provide a project lead to support the customer that will be used to oversee all aspects of the design and delivery of the Tax Specialist Programme. The customer and supplier will meet every month. It must be attended by the supplier's account manager, along with other supplier staff as appropriate to cover agenda items.
- The customer must receive a management report from the supplier prior to each meeting covering at least: an overview of Tax Specialist Programme performance, issues and risks; a summary of progress through the development of the exercises; a forward look summarising Tax Specialist Programme activity in the month to follow; and, communication opportunities and issues for the customer.
- Maintain a robust, effective, quality assurance and improvement regime consistent with the delivery of a high-quality, relevant, engaging and impactful Tax Specialist Programme.
- The supplier should be available to support customer queries by email/phone. Monday-Friday 8-6pm.

5. Service Levels and Key Performance Indicators (KPIs)

Whether in terms of quality or in terms of timeliness, service levels and Key Performance Indicators (KPIs) should be included in a specification. The Department must be able to measure the contractor's performance delivery and the specification must provide information of any service levels and/or KPIs that the contractor will be monitored against. The frequency of the monitoring must also be included to ensure a robust management regime.

Some service levels and KPIs are easily defined by reference to existing operations, SLAs etc. Where this is not the case, they need to be defined with users and can be informed by benchmarking information. It is important to set any performance measures at the right level:

- too high and they can be costly: the cost of meeting the higher performance level can be higher than the additional benefit obtained; and
- too low and users' expectations will not be met, and there may be a detrimental effect on the business.

KPIs should be clearly linked to the specification and payment regime to allow performance failure to be tracked and reflected in payment abatement.

The service levels and KPIs which will be monitored should be outlined in the Monitoring Schedule.

6. Contract Management and Review

Tier 4 contract management principles – Check requirement.

Optional Services required

Performance/Delivery Location/Premises

[redacted]

Standards

Quality Standards

Technical Standards

Disaster Recovery and Business Continuity

[redacted]

3. SERVICE PROVIDER SOLUTION

Service Provider Solution

Key Personnel of the Service Provider to be involved in the provision of the Goods, Services and Deliverables

[redacted]

Service Provider's inspection of the Premises and Infrastructure (where relevant)

[redacted]

4. PERFORMANCE OF THE GOODS AND/OR SERVICES AND DELIVERABLES

Implementation Plan and Milestones or e.g. delivery schedule (including dates for completion and/or delivery)

A draft template Implementation Plan as at the Commencement Date is set out below:

Milestone	Deliverables	Duration	Milestone Date	Customer Responsibilities (if applicable)	Delay Payments
September	launch and consultation		Week 3		
	prepare and deliver overview recommendations		Week 4		
October	create initial draft exercises by end of September		Weeks 1 to 3		
	full detailed exercise design		Week 4		
November	client exercise review and amends		Week 1 Week 2		
	exercise pilot		Week 3		
	amendments and assessor training design		Week 4		
December	client review and final loop for amendments		Week 1		
	final sign off		Week 2		

Critical Service Failure
(i) In relation to the Recruitment Assessment Services a Critical Service Failure shall mean a loss of for more than 24 hours accumulated in three (3) Month period, or 48 hours in any rolling twelve (12) month period.
Monitoring By way of written reports against the project timetable, outputs, KPIs and key milestones. We provide spend and billing reports at each review and/or project milestone linked to biling. **Management Information** Management Information to be provided in accordance with clause 7 of the Call-Off Terms on weekly basis in advance of the review meeting

5. CUSTOMER RESPONSIBILITIES

Customer's Responsibilities (where appropriate)

2 training events for up to 30 new assessors. Each event will be 1 day and will accommodate up to 15 delegates. The training will be delivered face to face and take place in HMRC offices in Nottingham.

Customer's equipment (where appropriate)

6. CHARGES AND PAYMENT

6.1 Contract Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. BACS))

[redacted]

6.2 Details of any Customer Rebate (if any) agreed in accordance with clause 11.5.

7. CONFIDENTIAL INFORMATION

The following information shall be deemed Commercially Sensitive Information:

[redacted]

8. AGREED AMENDMENTS TO THE CALL-OFF TERMS

The following amendments shall be deemed to be made to the Call-Off Terms:

9. PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. INTRODUCTION

1.1 The Service Provider shall not process any of the Customers personal data .

1.2 Any such further instructions shall be incorporated into this section 9 of the Master Contract Schedule.

Description	Details
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of Personal Data	
Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete unless requirement under union or member state law to preserve that type of data.	

10. PERSONAL DATA UNDER THE JOINT CONTROL OF THE PARTIES

Not applicable

HM Revenue & Customs

Security Plan Questionnaire - Low

To:	[redacted]
From:	[redacted]
Date:	[redacted]
Tender reference:	[redacted]
Tender title:	[redacted]

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
1b Please confirm your organisation and any subcontractors' will conform to the requirements set out in the ESPO Framework, and any Security Requirements recorded in the schedules and/or Order Form. [redacted]
1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the Data Protection act, and also confirm your data protection registration number. [redacted]
2 Physical Security (For requirements please see Appendix A – Physical Security)

2b Please provide details of the building where the service will operate from or HMRC data stored and describe the procedures and security in place to control access to premises and any areas holding HMRC data assets.
Please also include details of any automated access controls, alarms and CCTV coverage.

[redacted]

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.

[redacted]

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).

[redacted]

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.

[redacted]

[redacted]

5 Process Security (For requirements please see Appendix D – Process Security)

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.

[redacted]

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.

[redacted]

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.
Disposal of media	HMRC information assets must be sanitised in line with the Security Policy Framework.	

[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
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.	

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

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.

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	

Pricing Schedule – Redacted