Crown Commercial Service

Department for Work & Pensions

RM6100 Order Form – Lot 4

RM6100 Technology Services 3
Framework Schedule 4 Annex 1
Lot 4 Order Form

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Contract RM6100 dated 16th June 2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Contract**") and should be used by Buyers conducting a further competition under the Framework Contract.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Contract) consisting of this Order Form and the Call Off Terms. The Call Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Contract and copies of which are available from the Crown Commercial Service website Technology Services 3 - CCS (crowncommercial.gov.uk)
The agreed Call Off Terms for the Contract being set out as the Annex 1 to this Order Form. Where modifications to the Crown Commercial Services standard document have been made to accommodate the specific requirements and deliverables of this Contract these modifications are highlighted in light blue.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Term.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call Off Terms.

This Order Form shall comprise:

1. This document headed “Order Form”;
2. The following Attachments with reference to the corresponding Schedule in the Call Off Terms. Attachments to this Order Form either replace (i) an Annex to a Schedule in the Call Off Terms or (ii) a Schedule to the Call Off Terms in its entirety (for example, Attachment 2.1 (Services Description)):

Attachment to the Order Form	Schedule to the Call Off Terms
Attachment 2.1 (Services Description)	See Schedule 2.1 (Services Description)

Attachment to the Order Form	Schedule to the Call Off Terms
Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables)	See Schedule 2.2 (Performance Levels)
Attachment 2.3 (Environmental Requirements)	See Schedule 2.3 (Standards)
Attachment 2.4 (Information Management System)	See Schedule 2.4 (Security Management)
Attachment 3 (Buyer Responsibilities)	See Schedule 3 (Buyer Responsibilities)
Attachment 4.1 (Supplier Solution)	See Schedule 4.1 (Supplier Solution)
Attachment 4.2 (Commercially Sensitive Information)	See Schedule 4.2 (Commercially Sensitive Information)
Attachment 4.3 (Key Sub-Contractors)	See Schedule 4.3 (Key Sub-Contractors)
Attachment 4.4 (Third Party Contracts)	See Schedule 4.4 (Third Party Contracts)
Attachment 5 (Software)	See Schedule 5 (Software)
Attachment 6.1 (Outline Implementation Plan)	See Schedule 6.1 (Implementation Plan)
Attachment 6.2 (Test Success Criteria)	See Schedule 6.2 (Testing Procedures)
Attachment 7.1 (Charges)	See Schedule 7.1 (Charges and Invoicing) And document 13 PIP IT Managed Service Pricing Model
Attachment 7.2 (Maximum Payments on Termination)	See Schedule 7.2 (Payments on Termination)
Attachment 7.3 (Approved Benchmarkers)	See Schedule 7.3 (Benchmarking)
Attachment 7.4 (Financial Distress)	See Schedule 7.4 (Financial Distress)
Attachment 7.6 (Anticipated Savings)	See Schedule 7.6 (Anticipated Savings)
Attachment 8.1 (Representation and Structure of Boards)	See Schedule 8.1 (Governance)
Attachment 8.4 (Transparency Reports and Records to Upload to Virtual Library)	See Schedule 8.4 (Reports and Records Provision)
Attachment 9.1 (Notified Sub-Contractors)	See Schedule 9.1 (Staff Transfer)
Attachment 9.2 (Key Personnel)	See Schedule 9.2 (Key Personnel)
Attachment 11 (Processing Personal Data)	Schedule 11 (Processing Personal Data)

3. Annex 1 – Call Off Terms and Additional/Alternative Clauses.

The Order of Precedence shall be as set out in Clause 1.4 of the Call Off Terms being:

(a) the Framework, except Framework Schedule 18 (Tender);

(b) the Order Form and its Attachments (other than Attachment 4.1 (Supplier Solution) and its Annexes) and Schedule 2.2 (Performance Levels) and its Annexes;

(c) the Call Off Terms (including the Schedules and their Annexes) (other than Schedule 2.2 (Performance Levels) and its Annexes which is dealt with above in (b));

(d) Attachment 4.1 (*Supplier Solution*) and its Annexes (if any); and

(e) Framework Schedule 18 (Tender).

Where modifications to the Crown Commercial Services standard document were made in the Invitation to Tender to accommodate the specific requirements and deliverables of this Contract these are highlighted in cyan blue.

Section A

General Information

Contract Details	
Contract Reference:	ecm_10105
Contract Title:	PIP IT Managed Service
Contract Description:	This Contract is for a national managed IT service supporting PIP covering implementation and migration / transition services through to 1 August 2023, after which there will be 5 years of live operational running, through to 31 July 2028 to align with the operation of the Functional Assessment Service (FAS) contracts. FAS is being procured under a separate procurement for a single service from 1 August 2023 moving to one provider of all health assessments in a given geographical area.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	£31,028,545

Buyer details
Buyer organisation name
The Secretary of State for Work and Pensions (the Buyer also being referred to as "Department of Work and Pensions", "DWP" and "the Authority")
Billing address
Caxton House, Tothill Street, Westminster, SW1H 9NA
Buyer representative name
[redacted] Commercial Directorate
Redacted FOIA S40(1) personal data

Buyer representative contact details

[redacted] Redacted FOIA S40(1) personal data

Buyer Project Reference

Project 24319

Supplier details

Supplier name

Atos IT Services UK Ltd
DUNS Number 229500657
Company Number 1245534

Supplier address

MidCity Place 71 High Holborn London WC1V 6EA England

Supplier representative name

[redacted] Strategic Sales Executive – Large Deals Team

Redacted FOIA S40(1) personal data

Supplier representative contact details

[redacted] Redacted FOIA S40(1) personal data

[redacted] Redacted FOIA S40(1) personal data

Order reference number
A unique number provided by the supplier at the time of quote

Not applicable

Section B

Part 1 – Framework Lots (for multi-Lots only)

Not applicable

Part 2 – Contract Details

Term

Initial Term

Seventy-five (75) months from the Effective Date (comprising of a fifteen (15) month Implementation Services period followed by a sixty (60) month Operational Services period).

For the avoidance of doubt, to meet its known Operational Services requirements, the Buyer has elected to require fifteen (15) months of the maximum twenty-four (24) month Extension Period permitted under the Framework to be incorporated within the Initial Term.

Extension Period

Up to nine (9) months

Sites for the provision of the Services

The Supplier shall provide the Services from the following Sites**:**

Buyer Premises:

Not Applicable

Supplier Premises:

Delivery office: Daresbury Court 1 Evenwood Close (off Blackheath Lane) Runcorn Cheshire WA7 1SH
Head office: Second Floor, Mid City Place 71 High Holborn London WC1V 6EA

Third Party Premises:

Paragon
Delivery office: Paragon Customer Communications, 1 Hawkley Dr, Bradley Stoke, Bristol, BS32 0GE
Head office: Park House, Lower Ground Floor 16-18 Finsbury Circus, London EC2M 7EB
Company Registration 02788181

Buyer Assets
DWP Place Software
End User Devices (maximum of 5 laptops) for the Supplier to use for testing
Business Reply Envelopes directed to the DWP Main Opening Unit

Insurance

Third Party Public Liability Insurance: Not less than £10,000,000 (ten million pounds) in respect of any one occurrence, the number of occurrences being unlimited, but £10,000,000 (ten million pounds) any one occurrence and in the aggregate per annum in respect of products and pollution liability, and in all other respects the same as required under Part A to Annex 1 of Framework Schedule 14.

Professional Indemnity Insurance: Not less than £10,000,000 (ten million pounds) in respect of any one claim and in the aggregate per annum, and in all other respects the same as required under Part B to Annex 1 of Framework Schedule 14.

Goods
Not Applicable

Security Management – Option Part A or Part B

Security Management Schedule	Tick/insert "Y" as applicable
Part A – Security Assurance	☐
Part B – Security Accreditation	Y

The Part selected above shall apply to this Contract.

Section C

Part 1 – Additional and Alternative Buyer Terms

Alternative Clauses and Additional Clauses *(see Annex 3 of Framework Schedule 4) This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Alternative and Additional Terms and Conditions Lot 4*

Part A – Additional Clauses

Additional Clauses	Tick as applicable
C1: Collaboration Agreement	☐
C2: MOD Clauses	☐

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Alternative and Additional Terms and Conditions Lot 4 shall be incorporated into this Contract.

Part B - Alternative Clauses

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	☐
Northern Ireland Law	☐

Where selected above the Alternative Clauses set out in document RM6100 Alternative and Additional Terms and Conditions Lot 4 shall be incorporated into this Contract.

Part 2 - Additional Information Required for Additional Clauses Selected in Part 1

Additional Clause C1 (Collaboration Agreement)
Not Applicable

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Effective Date:

Not Applicable

Section D
Contract award

This Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Contract RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	[redacted] Redacted FOIA S40(1) personal data
Job role/title	**CEO Northern Europe & APAC**
Signature	[redacted] Redacted FOIA S40(1) personal data
Date	**18th May 2022**

For and on behalf of the Buyer

Name	[redacted] Redacted FOIA S40(1) personal data
Job role/title	**Chief Commercial Officer**
Signature	[redacted] Redacted FOIA S40(1) personal data
Date	**19th May 2022**

Attachments to this Order Form

This page is intentionally left blank

ATTACHMENT 2.1 – SERVICES DESCRIPTION

Table of clarifications

The following table details clarification questions raised during the further competition process with the Buyer's responses in the column headed "DWP Response", relevant to this Attachment 2.1. The provisions of this Attachment 2.1, and any related provisions in this Contract, shall be interpreted in accordance with the relevant DWP Response.

In this table, references to the "Authority" or to "DWP" are references to the Buyer.

Question Number	Question Classification	Question	DWP Response	Published
7	Notifications Printed	06 RM6100 Attachments - PIP IT Managed Service.docx Annex D - Notifications Printed (P29). Annex D indicates there are 6 x print notification types. How many different letter variants are there across those document types and across all 4 lots?	The Buyer will work with the supplier to agree the different letter variants for the print notification types. Currently there are in the region of 88 variants, (not including alternative formats) this will be kept under review and managed through	V3

			change control procedures.	
8	Notifications Printed	06 RM6100 Attachments - PIP IT Managed Service.docx Annex D - Notifications Printed (P29) Is there any difference between the letter templates used for each lot and if so, can you please explain the differences?	There are differences between the letter templates for Welsh language (Lot 2) and also some differences for NI (Lot 4) due to different legislation for a different authority.	v3
11	Notifications Printed	06 RM6100 Attachments - PIP IT Managed Service.docx Annex D - Notifications Printed (P29) Are there any additional inserts (Booklets or Leaflets) required for the Bulk Printing service other than the document types and if so, can we please have sight of these?	The Buyer will work with the supplier to agree any additional inserts which may be required, for example and not limited to: directions, information regarding	v3

			claiming expenses and support during the consultation.	
12	Notifications Printed	06 RM6100 Attachments - PIP IT Managed Service.docx Annex D - Notifications Printed (P29) Annex D indicates there are 3 x SMS notification types. How many different SMS message versions need to be created for sending?	The SMS timings and templates need to be configurable. There are currently PIP IT requirements covering 5 triggers for an SMS notification - receipt of referral, appointment booked, reminders (2) and cancellation. The Buyer will work with the supplier to agree the content.	3

51	Level 1 team size	What is the size of the team in Level 1 that will handle end user reported issues?	The DWP L1 team is circa 130. This team supports all of the DWP applications of which the PIP IT will be one of them.	v6
55	Annex D - Notifications Printed	The table in Annex D indicates a monthly volume of printed notifications of 150,000 per month. Approximately what % of these are expected to require a Business Reply Envelope to be included in the pack when despatched?	Approximately 50% of these are expected to require a Business Reply Envelope.	v7
56	Annex D - Notifications Printed	The ITT states the Supplier must "Deliver print outputs, as described in Annex D (Notifications), to the agreed collection point for the Buyer's nominated mail delivery provider in accordance with the despatch deadlines". Traditional process is that mail is collected from the print production facility by a mail provider -- can this be clarified please or, alternatively, advise where the agreed collection point will be for delivery charge costing purposes.	The agreed location will be the print production facility	v7
181	Accessibility Changes	044 In the ITT Further Instructions 13.1.2, you have referred to 1600 changes per annum in relation to Accessibility Management. Can you please provide some detail of the type and complexity of these changes to allow for costing. (Qualified as Access Management rather than Accessibility Management)	It is expected that year one of the contract will be a bedding in period with new technology and	13

			new users delivering a new service and therefore the type and volume of user access requests will reflect this. Given the situation, it is difficult to be precise in any estimates which is why the bidder has planned a true up exercise at the end of year 1. To assist estimation and costing please assume the following percentages based on 1600 changes for Year 1; 50% password resets, 30% new access requests, 20% leavers. We will work with the supplier to	

			drive the number of password resets to a minimum.	
177	ANNEX E – BASELINE VOLUMES	Can the DWP provide a breakdown of the 2,000 DWP user roles, so that we understand the work they will be undertaking and the level of application access that will be required. This is required to understand any impact on software licencing requirements.	Schedule 2.1 Annex E refers to 2000 users rather than 2000 user roles. These will primarily be DWP Case Workers who will be receiving calls from customers to ascertain the progress of their claim whilst in the AP space. So it is essentially a look up function. The access level required will be 'read only'.	13

190	Train the Trainer	Can DWP please confirm that the trainers who will attend the train the trainer course will be existing DWP staff who will already have the necessary context around DWP/PIP IT, the role of the assessment providers and the business processes that they follow? These will not be new teams or members of staff but existing DWP staff with PIP experience?	Trainers will be both DWP and Personnel already embedded in the incumbent PIP solutions	v13
191	Train the Trainer	Can DWP also confirm if any existing train the trainer material exists and can be developed as part of the training requirement? Or would DWP want brand new training material to be created?	It is the potential provider's responsibility to provide the requisite comprehensive trainer's training programme, material and environments for the new PIP IT Managed Service provision	v13
202	Licenses	Can The Authority confirm if they want: 1. All licences, including Third Party software license to be in there name 2. Can all licences be in a Bidders name providing they have the ability to novate them to the customer at end of contract or a termination event	DWP confirms option 2 as preferable	v15

216	Attachment 2.1 Services Description. 7.1.1. DWP Place.	"The Buyer shall provide the Supplier with the required level of access to the Buyer's Service Management Reporting tool DWP Place." Can we Buyer assume that DWP will provide the necessary licences for the Supplier's access?	The Buyer will provide supplier access	v17

1. DEFINITIONS

In this Attachment 2.1, the following definitions shall apply:

Term / Abbreviation	Definition
API Gateway	DWP hosted strategic solution for interfacing with DWP systems and services, acts as the single-entry point for DWP advertised Application Programme Interfaces.
Applications Hosting Services	The applications hosting services, which is an Operational Service, to be provided by the Supplier as described in Paragraph 4 of this Attachment 2.1.
Assessment Provider	The Functional Assessment Service (FAS) Suppliers who will use the PIP IT Managed Service for the delivery of Personal Independence Payment (PIP).
Assessment Provider Payment System	Assessment Provider system used to process payments.
Asset Register	The register of assets to be maintained by the Supplier pursuant to its obligations in Paragraphs 7.8.1 and 7.8.2 of this Attachment 2.1 (Services Description)
Baseline Volumes	The volumes for various aspects of the Supplier System that determine the overall sizing/capacity of the Supplier Solution, as detailed in Annex E (Baseline Volumes).
Bulk Print	Bulk print services as detailed in Paragraph 4 and Annex D of this Attachment 2.1.
Bulk Print Services	The bulk print services, which is an Operational Service, to be provided by the Supplier as described in Paragraph 5 of this Attachment 2.1.
Buyer Document Upload (currently DRS)	API to allow upload of documents to the DWP Document Repository System
Buyer System Interfaces	Interfaces which are required from the Supplier Solution to the Buyer Systems as detailed in Paragraph 3.4.1 of this Attachment 2.1.
Capacity Management Reports	Reports to be produced by the Supplier setting out the Capacity of the PIP IT systems as detailed in Annex B of this Attachment 2.1.
Capacity Management Services	The process responsible for ensuring that the capacity of the Services and the PIP IT Systems are able to deliver the KPIs in a cost effective and timely manner. Capacity Management considers all resources required to deliver the Services and the PIP IT Systems, and plans for the short, medium, and long term.
Claimant	A citizen who has applied for PIP benefit entitlement.
Claimant Expense	Expense allowances claimed by citizens

Term / Abbreviation	Definition
Conduct Feasibility Assessment Service	The conduct feasibility assessment Service, which is an Optional Service, as described in Paragraph 10 of this Attachment 2.1.
Configuration Management	
Design Changes Service	The design changes service, which is an Optional Service, as described in Paragraph 12 of this Attachment 2.1.
Design Deliverables	
Develop and Test Changes Service	The develop and test changes service, which is an Optional Service, as described in Paragraph 13 of this Attachment 2.1.
Disaster	The occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable for a period of 24 Hours, or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for that period.
Document Repository Service - DRS	The Document Storage IT System currently used by DWP to store correspondence and documentary evidence received in support of a claim for benefit.
DWP Place	The Buyer's Service Management Reporting tool
End User	Any person authorised by the Buyer to use the IT Environment and/or the Services.
Event	Shall be as defined in ITIL v4, as may be amended from time to time in any published updates to ITIL.
FAS Assessment Providers	The Functional Assessment Service (FAS) Suppliers who will use the PIP IT Managed Service for the delivery of Personal Independence Payment (PIP).
General Service Requirements	The Operational Hours for all Operational Services means the period between 08:00 and 20:00 Monday to Friday and the period between 09:00 and 17:00 on Saturday and Sunday.
General Practitioner Factual report (GPFR)	General Practitioner Factual report in connection with PIP.
Implementation and Release Service	The implementation and release service, which is an Optional Service, as described in Paragraph 14 of this Attachment 2.1.
Incident Management including Level 2 and Level 3	The process responsible for managing the lifecycle of all Incidents. The primary objective of Incident Management is to return the PIP IT Systems to Authority Users as quickly as possible.
Incidents	Any event that is not part of the normal operation of the PIP IT Systems or a Service and that causes, or may cause, an interruption

Term / Abbreviation	Definition
	to, or a reduction in, the quality of that PIP IT System or Service.
Integration Testing	Software testing where individual units / components are combined and tested as a group.
Interface Requirements	Interfaces which are required from the Supplier Solution as detailed at Paragraph 3.4 of this Attachment 2.1.
Invitation to Tender (ITT)	An invitation to submit tenders issued by the Buyer as part of an ITT Process.
Knowledge Application	Software product used to share knowledge about products and services. In DWP this role is fulfilled by the ServiceNow platform (DWP Place).
Major Incident Report	The report produced by the Supplier following a Severity 1 incident that details the root cause of the incident, and associated action items and recommendations, including lessons learnt.
Major Incidents	Incidents with significant business impact, requiring an immediate coordinated resolution.
Non-Production Environment	Those elements of the PIP IT Systems that are providing test, development, or standby services.
Operational Acceptance Testing - OAT	Operational Acceptance Testing evaluates the operational readiness of a software application prior to the release or production.
Operational Change Management	Changes to the Supplier Solution as detailed in Paragraph 7.11 of this Attachment 2.1.
Performance Levels	One or more metrics that define expected or achieved service quality. Expected Service Levels for this contract are shown in Schedule 2.2.
PIP	Personal Independence Payment (PIP) is a benefit which citizens can claim if they have a long term physical or mental health condition or disability; which helps fund additional costs for getting around or personal care.
PIP CS Personal Independence Payment Computer System	Computer System which manages the overall PIP customer journey. Used by the Buyer's to pay Claimant's benefits, store information about the claim and refer claimants for Medical Assessment.
Potential Provider	An organisation or individual that submits a Tender in response to the Further Competition Invitation.
Problem	A cause, or potential cause, of one or more incidents.
Problem Management	The practice of reducing the likelihood and impact of incidents by identifying actual and potential causes of incidents and managing workarounds and known errors.

Term / Abbreviation	Definition
Production	Those elements of the PIP IT Systems that are delivering live business applications to Authority Users of the Services, as opposed to those providing test, development, or standby services.
Production Environment	Th environments of the PIP IT Systems that are delivering live business applications to Authority Users of the Services.
Project Plan	Agreed by both parties a formal, approved document used to guide project execution and project control.
Recommend Service Packs and Patches	Software updates that can be applied to a software component to bring it to a level of support
Release	A version of the service or other configuration item, or a collection of configuration items, that is made available for use.
Release Management	The practice of making new and changed services and features available for use.
Release Management Service	The release management service as described at Paragraph 7.12 of this Attachment 2.1.
Release Plan	A rolling schedule of planned and potential Releases to the Supplier Solution as detailed in Paragraph 7.12.3 of this Attachment 2.1.
Requirements Analysis, Validation and Technical Options Service	The requirements analysis, validation and technical options service, which is an Optional Service, as described in Paragraph 11 of this Attachment 2.1.
RESTful API	A RESTful API is an architectural style for an application program interface that uses HTTP requests to access and use data
Request for Operation Change (RFOC)	Request For Operational Change ("RFOC") as detailed in Paragraph 9 of Schedule 8.2.
Root Cause Analysis	An activity that identifies the Root Cause of an Incident or Problem.
Service Continuity and Disaster Recovery Services	The service continuity and disaster recovery services, which is an Operational Service, to be provided by the Supplier as described in Paragraph 8 of this Attachment 2.1.
Service Desk	The single point of contact between the Supplier and the Authority's Users for the management of Incidents and Service Requests.
Service Levels	One or more metrics that define expected or achieved service quality. Expected Service Levels for this contract are shown in Schedule 2.2. (read as performance levels as well)
Service Management Reporting	Service management reporting, which is an Operational Service, to be provided by the

Term / Abbreviation	Definition
	Supplier as described in Paragraph 7.6 of this Attachment 2.1.
Service Management Services	The service management services, which is an Operational Service, to be provided by the Supplier as described in Paragraph 7 of this Attachment 2.1.
ServiceNow	Digital Product used for managing a service desk for the reporting & resolution of IT Incidents. In DWP this is also known as DWP Place.
Severity	The degree of the severity of an issue.
SMS Notification	Short Messaging Service notification as detailed in Paragraph 6 of this Attachment 2.1.
SMS Notifications Services	The SMS notifications services, which is an Operational Service, to be provided by the Supplier as described in Paragraph 6 of this Attachment 2.1.
SOAP	Simple Object Access Protocol.
Supplier Equipment Support Services	Support services for the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased, or loaned from the Authority) for the provision of the Services as detailed in Paragraph 7.3 of this Attachment 2.1
Tech Support	Common abbreviated form of Technical Support. In DWP Technical Support is the team who manage Service Desk functions.
Test Strategy	A strategy for the conduct of Testing as developed by the Supplier.
Vendor	Company providing a service or system (software / hardware) component used in the Supplier Solution.

2. INTRODUCTION

2.1 This Schedule, including its Appendices, details the Services that shall be provided by the Supplier pursuant to this Agreement in consideration for the Charges, and a set of Optional Services that may be commissioned by the Buyer from the Supplier as Changes in accordance with Schedule 8.2.

3. SERVICES DESCRIPTION

3.1 Implementation Services

3.1.1 The Implementation Services to be provided by the Supplier are set out in Annex C (Implementation Services) and Annex F (paragraph 9) to this Attachment 2.1 and as specified in Annex C to Attachment 4.1 question 4.5.

3.1.2 The Supplier shall provide the Implementation Services from the Implementation Services Commencement Date and in accordance with the Implementation Plan.

3.2 Operational Services

3.2.1 From the Operational Service Commencement Date, the Supplier shall provide the Operational Services detailed below:

3.2.1.1 Applications Hosting Services, as described in Paragraph 4;

3.2.1.2 Bulk Print Services, as described in Paragraph 5;

3.2.1.3 SMS Notifications Services, as described in Paragraph 6;

3.2.1.4 Service Management Services, as described in Paragraph 7;

3.2.1.5 Service Continuity and Disaster Recovery Services, as described in Paragraph 8;

3.2.1.6 General Service Requirements are detailed in Paragraph 9.

3.3 Optional Services

3.3.1 Where the Buyer/Supplier raise a Change Request requesting Optional Services from the Supplier, the Supplier shall provide the relevant Optional Service from the list detailed below:

3.3.1.1 Conduct Feasibility Assessment, as described in Paragraph 10;

3.3.1.2 Requirements Analysis, Validation and Technical Options, as described in Paragraph 11;

3.3.1.3 Design Changes Service, as described in Paragraph 12;

3.3.1.4 Develop and Test Changes Service, as described in Paragraph 13;

3.3.1.5 Implementation and Release Service, as described in Paragraph 14.

3.4 Interface Requirements

3.4.1 Buyer System Interfaces

3.4.1.1 The Supplier Solution shall support the following interfaces to the Buyer System, and shall ensure they continue to work in accordance with the existing interface definitions:

(a) PIP CS: Inbound files from PIP CS which provide initial referral details and updates from the Buyer relating to the referral;

(b) PIP CS: Outbound files to PIP CS which are change of circumstance in relation to referrals within the Supplier Solution;

(c) PIP CS: Inbound SOAP Interface to PIP CS via Buyer API Gateway, which provides details of the referral outcome (currently re-keyed into PIP CS);

(d) Buyer Document Upload Service (currently DRS): Outbound assessment reports (RESTful API) to transfer reports into the Buyer via the Buyer API Gateway;

3.4.1.2 Where there is a change to one of the Buyer System Interfaces the Supplier shall update the Supplier Solution to keep the interfaces current, as part of the Optional Service and following the Change Control Procedure as set out in Schedule 8.2.

3.4.2 Assessment Provider interfaces

3.4.2.1 The Supplier shall provide the following interfaces to the Assessment Provider(s) Payment Systems to allow the following:

(a) Claimant Expense fulfilment;

(b) GP Factual Report (GPFR) further evidence payment fulfilment.

3.4.2.2 The Supplier Solution is required to record the detail of expense claims and produce output for onward fulfilment but shall not be responsible for making the payments to the recipients.

3.4.2.3 The Supplier shall not be required to hold or process any card payments.

3.4.3 Supplier interfaces

3.4.3.1 The Supplier Solution shall provide the following interfaces:

(c) Management Information reports and raw data extracts (in a standard format agreed by the Buyer) should be made available to the Buyer and to third parties nominated by the Buyer.

3.4.4 In the event of a Disaster or component failure in respect of any of the Buyer System, Assessment Provider systems or Supplier Solutions referenced in Paragraphs 3.4.1, 3.4.2 or 3.4.3 above, the Supplier Solution shall have the capability to send or receive the relevant data via an alternative method to ensure continuity of information exchange.

3.5 Security Requirements

3.5.1 The Supplier shall comply with the requirements of Schedule 2.4 (Security Management) and Annex A to Attachment 4.1 (Information Security Questionnaire).

OPERATIONAL SERVICES (PARAGRAPHS 4 TO 9)

4. APPLICATIONS HOSTING SERVICES

4.1 The Supplier shall provide Services necessary to provide the Applications Hosting Services elements of the Supplier Solution which complies with:

4.1.1 the Buyer's requirements for the Applications Hosting Services as set out in Attachment 4.1 (Supplier Solution) and Annex C to Attachment 4.1 (see Non Functional Compliance and Information Requirements) and,

4.1.2 the Service Levels applicable to Applications Hosting Services as set out in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

4.1.3 the Baseline Volumes

4.2 The Supplier shall provide fully managed Applications Hosting Services for the Supplier Solution that are compliant with the requirements of Schedule 2.4 (Security Management) which can be based on either:

4.2.1 Supplier data centre hosting services from two (2) UK data centres, and which are geographically separated to protect the availability of Services in the event of a major outage at one of the centres; or,

4.2.2 Supplier's use of public cloud solutions such as 'Platform as a Service' (PaaS) or 'Software as a Service' (SaaS) provided that the Supplier can protect the availability of Services in the event of a major outage.

4.3 The Supplier Solution must include production environments and non-production environments (as detailed in Paragraph 4.4) as required for the Supplier to perform the Services.

4.4 Non-Production Environments

4.4.1 The Supplier shall maintain and provide non-production environments appropriate for it to perform the Services, including development, functional, regression, performance, accessibility, operational acceptance, service management and transition and prod-fix testing, using automated testing tools to inform quality management processes prior to releasing configuration changes into Production.

4.4.2 The Supplier shall maintain and provide a non-production environment which is appropriate for User functional testing.

4.4.3 The Supplier shall maintain and provide a training environment which meets the following requirements:

4.4.3.1 Enables the Buyer or their authorised representatives to perform training of Assessment Provider or End Users;

4.4.3.2 The training environment shall be available for access from any location using a Buyer approved and managed end user device;

4.4.3.3 The Supplier shall provide and maintain specific training data within the training environment to allow structured training of End Users. The training data will not be live data but it's purpose is to allow full training of End Users in all functions of the Supplier Solution. Training data should be capable of being restored prior to a scheduled training course, or at the request of the Buyer;

4.4.3.4 Unless otherwise agreed by the Buyer, all functional changes to the Supplier Solution shall be deployed into the training environment ahead of deployment to the production environment to enable the commencement of user training ahead of full release;

4.4.3.5 The Supplier shall be responsible for “Train the Trainer” type training at implementation, but not responsible for providing any training to End Users.

4.5 The Supplier Solution shall ensure the Supplier Solution is resilient with no single point of failure (including at the network access level) and shall achieve the Application Hosting Services KPIs in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

4.6 The Supplier Solution shall be compliant with and adhere to the standards, blueprints and frameworks specified in Schedule 2.4 (Security Management).

4.7 Backup and Restore

4.7.1 The Supplier shall ensure that Buyer Data is backed up in accordance with the backup and restore procedures detailed in Attachment 4.1 (Supplier Solution), and referenced in Schedule 8.6 (Service Continuity Plan and Corporate Resolution Planning) Part C Disaster Recovery and Annex C to Attachment 4.1 (see Non Functional Requirements Compliance).

4.7.2 The Supplier shall ensure that it is capable of restoring the Buyer Data to the point of the last committed transaction.

4.8 Data Retention and Archiving

4.8.1 The Supplier shall agree with the Buyer the strategy to archive Buyer Data to maintain system performance in accordance to order to meet with the Key Performance Indicator specified in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables);

4.8.2 All Buyer Data must have a retention period and must not be kept beyond the retention period specified in Attachment 11.

4.8.3 The destruction of Buyer Data at the end of the retention period must comply with Schedule 2.4 Paragraphs 12.1.4 and 12.1.5.

4.9 Access Management

4.9.1 The Supplier shall operationally manage the confidentiality, availability and integrity of Buyer Data and Buyer Software and Specially Written Software.

4.9.2 In relation to requests for access to the Supplier Solution (which shall be processed as Operational Changes), the Supplier shall:

4.9.2.1 Undertake all necessary identify validation processes prior to providing or modifying access;

4.9.2.2 Provide, remove or modify access in response to requests when appropriately approved, in accordance with the Key Performance Indicator specified in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables);

4.9.2.3 Monitor the lifecycle appropriateness of those access rights;

4.9.2.4 Log and track access;

4.9.2.5 Remove or restrict rights when requested or when a security risk has been identified.

4.9.3 The Supplier shall at all times maintain a list of the End Users and an audit trail of the activities performed pursuant to 4.9.2 above (including without limitation the source of any access requests, the identity validation processes performed, the approvals given and the checks made of the appropriateness of the approvals, and the changes made to the access rights of the End Users). The Supplier shall provide the Buyer with a copy of the list and the audit trail (or, where so requested, parts thereof) on request.

4.9.4 Where the Buyer or an End User reports that an asset has been lost or stolen, the Supplier shall minimise the Buyer's exposure to loss by:

4.9.4.1 Terminating communication services immediately after having been informed of the loss;

4.9.4.2 Remotely wiping portable access devices where technically feasible;

4.9.4.3 Removing or amending remote access accounts to prevent access from the lost or stolen asset.

4.9.5 The extent to which the Supplier can minimise the Buyer's exposure to loss will be dependent upon the time in which the Buyer notifies the Supplier of any loss or theft of a device upon it becoming aware of any such loss or theft. The Supplier shall perform the actions described in paragraph 4.9.4 above within one Working Day of notification by the Buyer, but will be unable to mitigate any loss incurred prior to that point.

4.9.6 Where the Buyer or an End User notifies the Supplier that a password requires resetting for a particular End User, the Supplier shall reset the password and notify the End User of the new password in accordance with the KPIs.

5. BULK PRINT SERVICES

5.1 The Supplier shall provide the Bulk Print Services detailed below:

5.1.1 Creation and fulfilment of the Bulk Print Services which comply with:

5.1.1.1 The functional and non-functional requirements for the Bulk Print Services set out in Annex C to Attachment 4.1 and,

5.1.1.2 The Bulk Print output specifications set out below.

(a) For examples of the types of printed output required see Annex D (Notifications).

(b) For volumes of printed outputs see Annex D (Notifications) and Annex E (Baseline Volumes).

5.1.2 Management and control of Bulk Print templates that support the multi-supplier Assessment Provider model, including the obligation on the Supplier to manage and control all required variants of print formats of each output template (e.g. Welsh language, large print, braille alternative variants).

5.1.3 Implement updates or amendments to Bulk Print templates (including all required variants of print formats of each output template, e.g. Welsh language, large print, braille alternative variants) as requested by the Buyer.

5.1.4 All Bulk Print output templates are deemed to be Documentation and therefore the Supplier shall ensure are uploaded to the Virtual Library.

5.1.5 Perform Bulk Print re-runs as agreed with the Buyer.

5.1.6 Sort Bulk Print outputs to minimise postage costs but ensuring all Bulk Print outputs are despatched using the postal tariff specified for each output type.

5.1.7 Create and issue Bulk Print output in accordance with despatch deadlines as specified in Bulk Print Services KPIs in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

5.1.8 Monitor information regarding volume of bulk print outputs and report monthly volumes by output and trends to the Buyer.

5.1.9 Procure, provide and manage all stationery required to undertake Bulk Printing, sorting and despatch.

5.1.10 Deliver print outputs, as described in Annex D (Notifications), to the agreed collection point for the Buyer's nominated mail delivery provider in accordance with the despatch deadlines. Collection by the Buyer's nominated mail delivery provider from the agreed collection point and onward distribution to the delivery address is not part of the Services.

6. SMS NOTIFICATIONS SERVICES

6.1 The Supplier shall provide the SMS Notifications Services as detailed below:

6.1.1 Creation and fulfilment of the SMS Notifications Services which comply with:

6.1.1.1 The functional and non-functional requirements for the SMS Notifications Services set out in Annex C to Attachment 4.1 and,

6.1.1.2 The SMS Notifications specifications set out below.

(a) For examples of the types of SMS notifications required see Annex D (Notifications).

(b) For volumes of SMS notifications see Annex D (Notifications) and Annex E (Baseline Volumes).

6.1.2 Management and control of SMS Notification templates that support the multi-supplier Assessment Provider model, including the obligation on the Supplier to manage and control Welsh language variants of each SMS Notification template.

6.1.3 Implement updates or amendments to SMS Notification templates (including all Welsh language variants of each SMS Notification template) as requested by the Buyer.

6.1.4 All SMS Notification templates are deemed to be Documentation and therefore the Supplier shall ensure are uploaded to the Virtual Library.

6.1.5 Create and issue SMS Notifications in accordance with despatch deadlines as specified in SMS Notification Services KPIs in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

6.1.6 Monitor information regarding volume of SMS Notifications and report monthly volumes by output and trends to the Buyer.

6.1.7 Pay all telephony / communications service provider costs associated with the transmission of all SMS Notifications.

7. SERVICE MANAGEMENT SERVICES

7.1 Service Management Reporting Tool

7.1.1 The Buyer shall provide the Supplier with the required level of access to the Buyer's Service Management Reporting tool DWP Place (Service Now) to enable:

7.1.1.1 The Supplier to view and manage incidents, problems and change requests raised via DWP Place. Examples of actions are listed below, but not limited to:

(a) Investigating and diagnosing incidents assigned from the Service Desk, Tech Support or via self-service via DWP Place.

(b) Ensuring problems are raised due to known errors, and investigating assigned problems through to root cause and resolution.

(c) Updating problems with new or updated known errors and workarounds.

(d) Ensuring any business facing knowledge article is produced for workarounds.

(e) Submitting appropriate request(s) for change (RFCs) to resolve problems ensuring any required fixes have been tested satisfactorily.

(f) Raising and managing changes in DWP Place, ensuring the change originator responds to any negative impacts or comments.

(g) Impacting other changes (via DWP Place) associated with the Service(s).

(h) Providing release collateral for all changes.

(i) Ensuring that knowledge articles and scripts are published and maintained in advance of a change being made or the Service being introduced.

(j) Effectively managing technical knowledge articles (created via Problem records, or via the Knowledge Application) throughout their lifecycle.

(k) Ensuring Event monitoring is in place for the Service(s) to provide the appropriate level of monitoring to meet business requirements.

7.1.1.2 The Supplier to produce the specified Service Management Reporting as detailed in section 7.6.

7.2 Software Management and Support

7.2.1 The Supplier shall provide the software management and support services listed below in respect of all Software and/or Buyer Software running within the Supplier Solution:

7.2.1.1 Proactive monitoring of systems to maximise system availability and reduce system failures;

7.2.1.2 Preventive maintenance based on monitoring and optimisation of software and data management, and reactive review and resolution of Incidents and error logs to detect problems and actions to correct these problems, in accordance with the KPIs defined in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables);

7.2.1.3 Management of any software including:

(a) software installations;

(b) software maintenance;

(c) software fixes and patches;

(d) software administration;

(e) system documentation;

(f) Full Vendor support of all software components in accordance with Vendor Recommended Service Packs and Patches (which shall be applied in a timely manner but in any event no later than ensuring all software is maintained to at least n-1, where “n” is the Vendor’s most recent patch set available).

7.2.2 Unless agreed by the Buyer, all software used in the Supplier Solution must be supported by the Vendor (for example should Microsoft cease to support a specific version of software then this

software must be replaced or upgraded to a supported version at no additional charge to the Buyer).

7.2.3 For any upgrades to software components of the Supplier Solution that are not covered by the Contract the Supplier shall raise a Change Request for consideration and approval by the Buyer.

7.3 Supplier Equipment Support

7.3.1 The Supplier shall provide the Supplier Equipment Support Services listed below:

7.3.1.1 The Supplier shall ensure that all Supplier Equipment is appropriately specified for the tasks it performs in delivery of the Services.

7.3.1.2 The Supplier shall ensure that all Supplier Equipment is fully supported and maintained and the Supplier shall procure that all Supplier Equipment used within the Supplier Solution is covered by the relevant Vendor's standard support service. Where the Supplier wishes to utilise a Vendor's extended support service, the Supplier shall be required to obtain the Buyer's prior written consent.

7.3.1.3 Proactive monitoring of systems to maximise system availability and reduce system failures;

7.3.1.4 Preventive maintenance based on monitoring and optimisation of Supplier Equipment and reactive review and resolution of Incidents and error logs to detect problems and actions to correct these problems, in accordance with the KPIs defined in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables);

7.3.1.5 Management of any Supplier Equipment including:

(a) installations;

(b) maintenance;

(c) fixes and patches;

(d) administration;

(e) system documentation.

7.3.1.6 Unless agreed by the Buyer, all Supplier Equipment must be supported by the Vendor. Where standard Vendor support is no longer available for any Supplier Equipment, or where the Buyer has not given consent that extended Vendor support can be utilised, the Supplier shall replace or upgrade the relevant Supplier Equipment so that Vendor support is available.

7.4 Data Management

7.4.1 The Supplier shall ensure that the Buyer Data retention policies are implemented and tested to ensure compliance within the scope of the IT services.

7.4.2 The Supplier shall ensure adherence to GDPR standards and guidelines in the processing of Buyer Data.

7.4.3 The Supplier shall adhere to the Security Management (Schedule 2.4) in the processing, storing and transfer of Buyer Data.

7.4.4 The Supplier shall adhere to Processing Personal Data (Schedule 11) in the processing, storing and transfer of Buyer Data.

7.4.5 The Supplier shall ensure, on an ongoing basis, the database of the Supplier Solution is optimised and tuned to meet the KPIs specified in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables) and the Buyer Data is correct and fit for purpose.

7.5 Capacity Management and Planning

7.5.1 The Supplier shall provide the following capacity management and planning Services:

7.5.1.1 The Supplier shall capacity plan for the business usage demand and volumes provided by the Buyer on at least a quarterly basis.

7.5.1.2 The Supplier shall ensure that agreed future business requirements for Services are considered, planned and implemented within appropriate timescales.

7.5.1.3 The Supplier shall provide all Capacity Management Reports to the Buyer (on the relevant frequency) as detailed in Annex B (Service Management Reports) and Attachment 8.4.

7.5.1.4 The Supplier shall analyse utilisation trends within the scope of the Services, including infrastructure and applications, and projecting their potential impact on future known capacity requirements; and

7.5.1.5 The Supplier shall monitor actual volumes against each of the Baseline Volumes set out in Annex E (Baseline Volumes), and shall notify the Buyer as soon as reasonably practicable where it anticipates that any of the Baseline Volumes are likely to be exceeded given trends or its knowledge of the business activities of the Buyer.

7.6 Service Management Reporting

7.6.1 The Supplier shall provide all monthly reports, detailed within Annex B (Service Management Reports) electronically to the Buyer by the 10th Working Day of the following month.

7.6.2 The Supplier shall ensure that all reports are an accurate reflection of the Services performed during the relevant Service Period.

7.6.3 The Supplier shall provide a review of all Service performance as input to the relevant governance boards as detailed in Schedule 8.1 (Governance).

7.6.4 The Supplier shall provide agreed reports electronically to the Buyer.

7.6.5 The Supplier shall provide all other reports as set out and in accordance with Schedule 8.1 (Governance).

7.6.6 Standard reports. The Supplier shall provide to the Buyer monthly reports containing the following information:

7.6.6.1 The Performance Monitoring Report as defined in Schedule 2.2;

7.6.6.2 Metrics including, but not limited to:

(a) number of Problems;

(b) volume of Incidents created by Severity;

(c) volume of Incidents closed by Severity; and

(d) number of RFOCs both in total and by type, including whether they were performed or not.

7.6.6.3 A Major Incident Report and Root Cause Analysis for Major Incidents.

7.6.6.4 Overview of changes deployed into Production (broken down into changes which required regression and changes which didn't require regression).

7.6.6.5 Capacity Management Reports shall be agreed between the Supplier and the Buyer post contract award.

7.7 KPI Management

7.7.1 The Supplier shall:

7.7.1.1 be responsible for the management of the KPIs as defined in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables) for the delivery of the Services;

7.7.1.2 maintain and improve the quality of the Services through a constant cycle of agreeing, monitoring, reporting and reviewing Services achievements; and

7.7.1.3 instigate actions to eradicate unacceptable performance levels in providing the Services.

7.7.2 The Supplier's responsibilities for the provision of KPI management in relation to the Services are:

7.7.2.1 measuring and reporting of the KPIs actually achieved against target as outlined in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

7.8 Configuration Management

7.8.1 The Supplier shall implement and maintain an Asset Register and a library of other Sub-contracts and other relevant agreements (including relevant software licences, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services as referenced in Schedule 8.5 Paragraph 2.1 (a) and (b).

7.8.2 Asset Register

7.8.2.1 The Supplier shall provide to the Buyer an Asset Register with details for all assets which form part of the Supplier Solution which are procured after the Effective Date which are Exclusive Assets.

7.8.2.2 The Asset Register shall cover hardware assets and software to provide full transparency enabling the Buyer to adhere to IFRS in relation to its accounting policy for assets.

7.8.2.3 The Supplier shall provide the first version of this Asset Register to the Buyer within one (1) month of the Operational Services Commencement Date, and shall provide quarterly updates thereafter.

7.8.2.4 The Supplier shall ensure that the Asset Register is in the form set out at Annex A (Asset Register, Software Compliance Report, Configuration Database), and is completed in accordance with the notes set out in that annex.

7.8.2.5 The Supplier shall provide a quarterly report to the Buyer regarding software licence compliance for any and all Supplier or Supplier sub-contractor licensed software used within the Supplier Solution (the "Software Compliance Report"). Such reports shall be in the format set out in Annex A (Asset Register, Software Compliance Report, Configuration Database), and the Supplier shall complete the reports such that all relevant columns are fully completed and with such information as the Buyer reasonably requires in order to demonstrate that it is complying with the terms of the relevant licence.

7.8.3 The Supplier shall implement and maintain a configuration database in a format to be agreed to the Buyer post contract award and in-line with Schedule 8.5 Paragraph 2.1 (b). This will form a key component of any exit strategy / business continuity plan.

7.8.4 Incident Management

7.8.5 The Supplier shall provide Level 2 and Level 3 Incident Management for all areas of the Supplier Solution and the Services via the Buyer's Service Management tool DWP Place (Service Now). The facilities provided by the Incident Management Service are:

7.8.5.1 timely Incident detection and recording;

7.8.5.2 accurate classification and initial investigation;

7.8.5.3 timely and accurate allocation of Incidents;

7.8.5.4 ownership and monitoring of all Incidents through to successful Resolution;

7.8.5.5 ensuring all updates are recorded in the Buyer's Service Management tool DWP Place (Service Now) in a timely manner;

7.8.5.6 allocating to multiple support teams for parallel investigation where required and co-ordinating any joint investigations between support teams;

7.8.5.7 manual and automatic escalations throughout the Incident lifecycle to the point of Resolution and closure;

7.8.5.8 co-ordinate and produce a Major Incident Report and Root Cause Analysis for Major Incidents.

7.8.6 Incident Resolution KPIs are measured from the point of when the first ticket is logged within DWP Place.

7.9 Problem Management

7.9.1 The Supplier shall provide Problem Management to the Buyer. This Service is designed to improve the delivery of Services by ensuring the Resolution of Problems and identifying trends that may impact on future performance. The features of Problem Management are:

7.9.1.1 identify, record and classify Problems;

7.9.1.2 prioritisation of Problems based on impact to KPIs as defined in Schedule 2.2 (Performance Levels) and the probability of reoccurrence;

7.9.1.3 manage the investigation of Problems and coordinate Root Cause Analysis;

7.9.1.4 document recommendations;

7.9.1.5 agree and document follow-up actions, based on recommendations;

7.9.1.6 managing the follow-up actions to completion within agreed timescales;

7.9.1.7 reporting progress of follow-up actions to the Buyer at agreed regular intervals;

7.9.1.8 initiate, complete and present to the Buyer lessons learned reviews, as appropriate;

7.9.1.9 analyse Incidents and Problems to identify trends and implement remedial action as required; and

7.9.1.10 produce management information based on Problem Management data.

7.9.2 This Service is to be used for all Problems affecting delivery of Services to the Buyer.

7.10 Event Management

7.10.1 The Supplier shall detect Events on the Supplier Solution, analyse them and determine appropriate control activity, and maintain appropriate logs within DWP Place (Service Now) regarding events and their outcomes.

7.10.2 Where the Event results in, or has the potential to result in, an unplanned interruption to a Service or a reduction in the quality of a Service, the Supplier shall raise an Incident and manage resolution in accordance with the Incident Management service (Paragraph 7.8.4).

7.10.3 The Supplier shall maintain data in relation to Events within DWP Place (Service Now) such that it can evidence and report on performance against the KPIs.

7.11 Operational Change Management

7.11.1 The Supplier shall perform Operational Changes to the Supplier Solution as required and/or agreed. The Supplier shall perform such Operational Changes in order to deliver the Services and achieve the KPIs, and with the aim of offering operational flexibility to the Buyer where this can be offered without unreasonable risk to the Services or the Supplier Solution.

7.11.2 Operational Change management processes shall be undertaken within the principles defined in Paragraph 9 of Schedule 8.2 (Change Control Procedure). The Supplier shall document and operate the processes relating to Operational Changes, and shall make the documentation of these processes available to the Buyer and the relevant Buyer's Sub-Contractors who may need to raise or consider Operational Changes. Such processes shall cover:

7.11.2.1 submission, recording and processing of RFOCs, including any quality assurance performed on RFOCs;

7.11.2.2 the process for obtaining impact statements from all groups potentially impacted by an Operational Change, which shall include the Supplier providing a summary view of all impacts to any change approval board;

7.11.2.3 the process and meetings used to agree and schedule Operational Change, including definition of any key stakeholders within the Supplier and the Buyer, whose agreement must be obtained before particular types of Operational Change can be agreed or scheduled;

7.11.2.4 building, testing and implementation of the solution to support requested Operational Change if applicable;

7.11.2.5 monitoring, reporting and closure of RFOCs;

7.11.2.6 communication to the Buyer; and

7.11.2.7 management information reporting.

7.11.3 Where an Operational Change is made, the Supplier shall amend any relevant documentation such that the documentation remains an accurate description of the Supplier Solution.

7.12 Release Management

7.12.1 The Supplier shall be responsible for the management of any and all Releases to any environment used to provide the Services.

7.12.2 The Supplier shall provide planning, testing and rollout of all software and hardware Releases and patches to minimise any adverse or unplanned consequences of a Release.

7.12.3 The Supplier shall create and maintain rolling schedule of planned and potential Releases to the Supplier Solution (the "Release Plan") which shall be agreed with the Buyer. Changes to the Release Plan shall be agreed through the Change Procedure.

7.12.4 The responsibilities of the Supplier in providing the Release Management Service include:

7.12.4.1 planning and overseeing the rollout of software and related hardware, and designing and implementing efficient procedures for the distribution and installation of changes;

7.12.4.2 ensuring all relevant Release documentation is produced and accurate;

7.12.4.3 ensuring adequate levels of testing are conducted (including supporting any Buyer testing);

7.12.4.4 ensuring that security is not compromised as a result of deployment of Releases;

7.12.4.5 ensuring that tested roll-back plans are documented for all Releases;

7.12.4.6 ensuring any change is traceable, secure and that only correct, authorised and tested versions are installed;

7.12.4.7 communicating and managing expectations of the Buyer (through communication to a single point of contact either within the Buyer or such third party as the Buyer may specify) during the planning and rollout of new Releases; and

7.12.4.8 liaising with Operational Change Management to implement new software and/or hardware Releases and to ensure that the Asset Register and/or the other Sub-contracts and other relevant agreements are updated.

7.12.5 A Release may consist of any combination of hardware, services, software, firmware and documents.

7.12.6 The Supplier shall be responsible for Configuration Management in support of Release Management, which shall cover:

7.12.6.1 identification of the level of detail required for appropriate management;

7.12.6.2 discovery and maintenance of accurate information on the Supplier Solution, the Non-Production Environments, their components and their documentation;

7.12.6.3 control to ensure that only authorised, identified components are accepted and maintained; and

7.12.6.4 roles and responsibilities of relevant stakeholders.

7.13 Availability Management

7.13.1 The Supplier shall perform the Services such that each Supplier Solution is available for the End Users to at least the relevant Availability KPI, but shall make the Supplier Solution available throughout the Operational Hours, save where the Buyer has agreed to Permitted Maintenance through the Operational Change Procedure.

7.13.2 The Supplier shall make access to relevant Software or Buyer Software available outside of the Operational Hours where the Buyer requests such access through the Operational Change Procedure.

7.13.3 The Supplier shall undertake ongoing monitoring and measurement for the availability of all aspects of the Services.

7.13.4 Responsibilities of the Supplier in providing Availability Management relating to the Services are:

7.13.4.1 optimising Service availability;

7.13.4.2 monitoring of service and exception reporting;

7.13.4.3 ensuring KPIs are met by monitoring service availability levels against KPIs, and monitoring external supplier serviceability achievements;

7.13.4.4 collecting, analysing and maintaining availability data; and

7.13.4.5 working with the Buyer to agree the schedule for change to minimise maintenance and upgrade time windows.

7.13.5 Planned unavailability of the Supplier Solution or any part thereof shall be performed in such a manner as to minimise the disruption of the Buyer business processing. The Supplier shall not unreasonably request Planned Maintenance during the Operational Hours. The Supplier shall notify the Buyer of any Planned Maintenance outside the Operational Hours.

7.14 Continuous Improvement

7.14.1 The Supplier shall have an ongoing obligation throughout the term of the contract to identify new or potential improvements to the Services (in accordance with Clause 8 - “Service Improvements” of the Call Off Terms).

7.14.2 In addition to Clause 8, following the report to Programme Board at the end of the first 12 months, the Supplier shall create and agree with the Buyer, within 1 calendar month, a Continuous Improvement Plan for the delivery of the agreed Service Improvements, for the following 12 months, which have been agreed with the Buyer, in accordance with the Change Control Procedure.

7.14.3 The Supplier shall report progress against the delivery of the Continuous Improvement Plan for Service Improvements, at the end of each Service Period, along with recommendations of any improvements identified in accordance with the Change Control Period.

7.14.4 Changes to the way in which the Services are to be delivered must be brought to the Buyer’s attention and agreed prior to any changes being implemented.

7.15 Service Management Information Reporting

7.15.1 The Supplier shall use the Buyer’s Service Management Reporting tool DWP Place (Service Now) to produce the specified Service Management Reporting as detailed in Paragraph 7.6.

7.15.2 The Supplier shall provide all Monthly reports, detailed within Annex B (Service Management Reports) electronically to the Buyer by the 10th Working Day of the following month.

7.16 Documentation

7.16.1 All Documentation shall be published in appropriate form(s) and uploaded to the Virtual Library. Documentation must be at a level appropriate with Good Industry Practice.

7.16.2 All Documentation shall be managed, maintained and kept up to date by the Supplier at all times.

7.16.3 All Documentation shall be subject to formal version control.

7.16.4 Where a change to any Documentation has security relevance the Supplier must bring the change to the attention of the Buyer and gain approval before the change is implemented.

8. SERVICE CONTINUITY AND DISASTER RECOVERY SERVICES

8.1 The Supplier shall ensure the Supplier Solution (covering the scope of all Operational Services) shall comply with all service continuity and disaster recovery requirements detailed in:

8.1.1 Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables); and,

8.1.2 Schedule 8.6 (Service Continuity Plan and Corporate Resolution Planning).

9. GENERAL SERVICE REQUIREMENTS

9.1 The Operational Hours for all Operational Services means the period between 08:00 and 20:00 Monday to Friday and the period between 09:00 and 17:00 on Saturday and Sunday.

OPTIONAL SERVICES (PARAGRAPHS 10 TO 14)

10. CONDUCT FEASIBILITY ASSESSMENT

10.1 In the event that the Parties agree (such agreement not to be unreasonably withheld or delayed) that a Change Request Impact Assessment cannot be provided in relation to a Change Request due to the complexity or range of options involved, the Buyer may request the Optional Service “Conduct Feasibility Assessment”. Where the Buyer so requests, the Supplier shall provide the Feasibility Assessment by the date specified in the agreed request. The Supplier shall provide in each Feasibility Assessment:

10.1.1 The impact of the change on the existing Services;

10.1.2 The System that the Supplier would recommend for achieving the Change Request, and any options for delivery (with an assessment explaining why the recommended option is preferred);

10.1.3 The estimate for delivery of the change and for any option, which shall be based on the Rate Card set out in Annex 1 of Schedule 7.1;

10.1.4 The plan for delivering the change (and for any options).

11. REQUIREMENTS ANALYSIS, VALIDATION AND TECHNICAL OPTIONS

11.1 The Supplier shall provide the following activities as part of delivering this Optional Service:

11.1.1 Analysis and validation of the Buyer's requirements and the conceptual design of the proposed solution for the requested change, in accordance with the timescales agreed in the Change Authorisation Note;

11.1.2 Identification of gaps in functional requirements and potential challenges to typical non-functional requirements;

11.1.3 Production of Test Success Criteria for the functional and non-functional requirements;

11.1.4 Development of a proposal for a high level solution and delivery plan to meet the Buyer's requirements;

11.1.5 Where required, production of an appraisal of the full range of technical options, including a recommended option with the appropriate rationale, which meets the Buyer's requirements and in accordance with the agreed timescales. For instance, the appraisal may include details of COTS products required, bespoke application development and/ or the re-use of existing applications;

11.1.6 Formulation of a Test Plan for the requested change to the Supplier Solution. It is likely that different approaches to mitigating risk may exist, depending upon the changes to the service.

11.1.7 As part of the Requirements Analysis, Validation and Technical Options the Supplier may:

11.1.8 Propose changes to the Buyer's requirements to assist the Buyer in the standardisation of its requirements.

11.1.9 Notify the Buyer if fulfilling the Buyer's requirements unchanged would or may have an adverse impact on the Production Environment and/or the business processes of the Supplier Solution.

11.1.10 Propose to the Buyer alternatives to the Buyer's requirements that would mitigate any adverse impact on the Production Environment.

12. DESIGN CHANGES

12.1 The Supplier shall produce and deliver to the Buyer the amended and any additional Design Deliverables which meet and comply with the Buyer's requirements and the Standards (except to the extent that an exemption is agreed in writing by the Buyer) by the Milestone Date set out in the applicable Change.

12.2 Where the Buyer requests, the Supplier shall meet with the Buyer or shall respond to written queries in order to demonstrate how the Design Deliverables meet the Buyer's requirements and the Standards.

12.3 The Supplier shall document a project Test Plan defining how a proposed change to the Supplier Solution will be tested, the environments that will be used for testing and the entry and exit criteria for each test phase. Such project Test Plan will cover each phase of testing defined in the Test Strategy (as provided by the Buyer from time to time) unless the Buyer agrees in writing with a recommendation that a particular phase is not required given the scale or nature of the change, and the entry and exit criteria for each phase shall be suitable to achieve the purpose of that phase as defined in the Test Strategy. The Supplier shall seek input from and take account in the project Test Plan of how the Buyer (and if relevant the FAS Assessment Providers) intends to run any test phases for which it is responsible.

12.4 The Supplier shall provide an initial draft of the project Test Plan for review by the Buyer (and if relevant the FAS Assessment Providers), and an amended draft taking account of any comments made in this review by the Milestone Date set out in the applicable Change.

13. DEVELOP AND TEST CHANGES

13.1 The Supplier shall create, modify or enhance the Supplier Solution and its associated documentation such that the Supplier Solution meet the additional requirements and is in accordance with the amended or additional Design Deliverables by the Milestone Date set out in the applicable Change.

13.2 The Supplier shall produce and agree with the Buyer a test phase plan for each test phase for which it is responsible under the project Test Plan. In proposing test phase plans, the Supplier shall propose a level of testing which is proportionate to the scale and type of change being made to the Supplier Solution.

13.3 The Supplier shall review and contribute to any test phase plans being created by the Buyer or any third party for test phases for which they are responsible.

13.4 The Supplier shall perform testing in accordance with the project test strategy and all test phase plans, and manage defects and other issues arising during testing in accordance with the project test strategy.

13.5 The Supplier shall develop and demonstrate to the Buyer test components (including, but not limited to, test modules, test plans, test documents, test scripts and test data) to support effective testing of the amended Supplier Solution, and ensure, insofar as practicable, these products automate and optimise the performance of testing.

13.6 The Supplier shall produce and deliver test completion reports to demonstrate to the Buyer that the amended Supplier Solution and its associated code and documentation meet and comply with the requirements and the Design Deliverables, and meet the exit criteria for that test phase.

13.7 The amended Supplier Solution delivered pursuant to Paragraph 13.1 above shall meet the quality and Test Success Criteria as agreed with the Buyer and the exit criteria for each test phase set out in the project Test Plan and in each test phase plan.

13.8 The Supplier shall update the Supplier Solution training environment(s) by the Milestone Date in the applicable Change such that any training Services to be provided by the

Supplier are appropriate to train the End Users in the use of the amended Supplier Solution.

14. IMPLEMENTATION AND RELEASE

14.1 The Supplier shall plan, manage and perform the appropriate activities to release a change to the Supplier Solution into the Production Environment, and develop and manage an Implementation Plan to enable the successful delivery of the change.

14.2 As part of this Optional Service, the Supplier shall provide a number of detailed activities, including:

14.2.1 Prepare the necessary Deliverables, e.g. infrastructure changes, executable code, reference data configuration changes and supporting application artefacts and installation instructions, to ensure that they are ready for release;

14.2.2 Perform planning and agree the support arrangements for the build and installation of the Deliverables, in accordance with the Project Plan;

14.2.3 Develop a Project Plan for the change to the Supplier Solution, which reflects the Test Success Criteria for a successful release, and review the plan with the Buyer;

14.2.4 As requested by the Buyer, assist the Buyer in completing an early review of operational risk of the change to the Supplier Solution, as part of an operability review.

14.2.5 Manage the implementation and release of the change to the Supplier Solution;

14.2.6 Support changes to business products that have been developed for the Supplier Solution, e.g. training environments, user guidance, and learning and development material;

14.2.7 Where requested by the Buyer, checking of business outputs as required following implementation;

14.2.8 Where Defects identified in testing have been implemented into the Production Environment by agreement with the Buyer, raise an Incident for each Defect in accordance with the Service Management Service (Paragraph 7.8.4);

14.2.9 Ensure that a lessons learned review is held to ensure that any agreed corrective action is taken at the earliest opportunity.

ANNEX A – ASSET REGISTER, SOFTWARE COMPLIANCE REPORT, CONFIGURATION DATABASE

1. ASSET REGISTER

The Asset Register shall record details of the assets that make up the Supplier Solution and shall be captured in the table below and extends the requirement specified in Schedule 8.5 (Exit Management):

a) make, model and asset / serial number;

b) ownership and states as either Exclusive Assets or Non-Exclusive Assets;

c) Net Book Value;

d) physical location;

e) use (including technical specifications)

f) estimated life expectancy

g) condition and maintenance history, including repairs and downtime

Make / Manufacturer	Model Number	Asset / Serial Number	Exclusive / Non-Exclusive Asset	Net Book Value	Physical Location	Estimated Life Expectancy	Condition	Maintenance History
ATOS have no hardware assets. For software assets see Attachment 5.								

2. SOFTWARE COMPLIANCE REPORT

The Supplier shall be expected to maintain a list of software and their associated licenses used in the Supplier Solution and provide the Buyer a quarterly “Software Compliance Report” containing, but limited to, the Vendor of the software, the software, the version of the software and details of the license agreement. The format of the report shall be agreed with the Supplier post Effective Date.

3. CONFIGURATION DATABASE

The Supplier shall agree the format of the configuration database with the Buyer post Effective Date.

ANNEX B – SERVICE MANAGEMENT REPORTS

Service Reporting Items - Produced Monthly

Incident Reports

- Volume of Incidents Closed in Last 13 Months (All Tickets)
- P1 & P2 Incidents Closed – Detail
- Volume of Incidents Opened in Last 13 Months (All Tickets)
- P1 & P2 Incidents Opened - Detail
- SLA% Performance of All Incidents
- Volume of Incidents Opened by the Top 10 Incident Categories (All Tickets)
- Volume of Incidents Opened by the Top 10 Incident Categories (13 Months)
- Account Tickets Closed Last month by Category
- Volume of Incidents Closed by the Top 10 Root Causes in Month
- Volume of Incidents Closed by the Top 10 Root Causes (13 Months)

Capacity Reports

- Capacity reports to be agreed post contract.

ANNEX C – IMPLEMENTATION SERVICES

Redacted FOIA S43 Commercial Interest

[redacted]

[redacted]

[redacted]

ANNEX D – NOTIFICATIONS

Notifications – Printed

1. Letters shall be printed and despatched via Buyer's nominated mail delivery provider in accordance with the despatch deadlines, as specified in Bulk Print Services KPIs in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

2. Standard printed outputs should be double sided (duplex), monochrome printing

3. Alternative version outputs must be available for all printed output and include:
   - Braille
   - Large Print
   - Welsh Language
   - Audio CD

   For Braille, Large Print and Audio CD formats these represent less than 1% of volume.

Notification Types

Type	Number of Pages	Volumes per Month
Appointment Letters (Various Types e.g. F2F, VA, TA)	6-10	80,000
Complaints Letter (Various Types)	1	1,500
Claimant Expense letters (Various Types)	1	6,000
Appointment Cancellation Letters	1-2	1,500
GP Factual Report (GPFR) further evidence Letter (Various Types)	5-8	50,000
Other various notifications	1-4	11,000

Average volumes per month.

Notifications – SMS

1. SMS messages shall be despatched in accordance with the despatch deadlines, as specified in SMS Notifications Services KPIs in Attachment 2.2 (Key Performance Indicators and Subsidiary Performance Indicators Tables).

2. Alternative version outputs must be available for all SMS output and include:

    - Welsh Language

SMS Notification Types

Type	Volumes per Month
Appointment Created (Various Types e.g. F2F, VA, TA)	80,000
Appointment Reminder (Various timings)	160,000
Other various SMS	140,000

Average volumes per month.

ANNEX E – BASELINE VOLUMES

User Base

The Supplier Solution should be sized to accommodate the following user base

User Functions	Number of System Users	Concurrency
Assessment Provider User	4,500	3,500
DWP User	2,000	1,500
Training User	250	200

Average volumes per month.

Interface Transactions

Transactions on interface…	Number per Month
IF6: Inbound SOAP Interface to PIP CS via Buyer API Gateway, which provides details of the referral outcome (currently re-keyed into PIP CS).	120,000
IF7: Inbound files from PIP CS which provide initial referral details and updates from the Buyer relating to the referral.	141,000
IF8: Inbound IF6 SOAP Interface to PIP CS via Buyer API Gateway, which provides details of the referral outcome (currently re-keyed into PIP CS).	7,000
Uploads to Document Repository	120,000
AP systems (expense payments)	14,000

Average volumes per month.

SMS / Printed Notifications

Type	Number per Month
Printed Notifications	150,000
SMS	380,000

Average volumes per month.

Audits
Approximately 18,000 cases per month are selected for Audit. Audit selection criteria can vary between Assessment Providers but this figure should be taken as a baseline indicator.

Expense Payment Creation

Type	Number per month
Claimant / Companion Expenses	5,000
Further Evidence from GPs	9,000

Average volumes per month.

Appointments Booked

An average of 80,000 appointments are booked each month, these can be either automated or manual.

Non-Notification Documents Generated / Stored

Type	Number Created per Month	Overall Stored
PA1 – FME Needed	60,000	1,440,000
PA2 – Terminal Ill Report	3,000	72,000
PA3 – Paper based Report	9,000	216,000
PA4 – Face to Face Report	55,000	1,320,000
PA5 – Supplementary Advice Note (no outcome change)	1,800	43,200
PA6 – Supplementary Advice Note (outcome change)	900	21,600
PA7 – Harmful Information Note	10,000	240,000

Average volumes per month.

ANNEX F – APPENDIX B SPECIFICATION

Table of clarifications

The following table details clarification questions raised during the further competition process with the Buyer's responses in the column headed "DWP Response", relevant to this Annex F - Appendix B Specification. The provisions of this Annex F, and any related provisions in this Contract, shall be interpreted in accordance with the relevant DWP Response.

In this table, references to the "Authority" or "DWP" are references to the Buyer.

Question Number	Question Classification	Question	DWP Response	Published
57 (was 93)	Design Diagram	Can the authority please tell us if the architecture design diagram on page 16 (section 7.19) of the "Appendix B Specification" is an "as-is" architecture or a future architecture with a deployment activity on the authority. If it is a future design, then can the authority please indicate when this infrastructure will be built, and will it be available to meet the timelines of the MVP and migration activities, as mentioned in the ITT.	The diagram is a high level view of the future design. IT incorporates much of the infrastructure and capabilities which already exist within the Authority. One exception is the IF6 interface will need to be provisioned externally on the API Gateway but it is envisaged this will be completed mid 2022	v7
60 (was 96)	Functional Questions	The Authority's CQ 45 explained that 'use of the DWP IF6 interface via the DWP API Gateway will be deemed as a mandatory requirement to update PIPCS of assessment outcomes'. The diagram on process flow on page 12 of the Appendix B Specification was also updated to reflect this clarification, and now clearly shows the automated transmission of the	IF6 will be used for all scenarios listed, with the exception of '4' as we are not clear what this scenario is.	v7D

		completed assessment report and thus no admin user action during the closure process. This clarification is helpful, but although the diagram is clear and unambiguous, it is limited to showing what might be described as the ‘sunny day scenario’ of assessment report completion. Some uncertainty remains around other scenarios and the scope of the term 'assessment outcome'. This is, in part, because the IF6 interface definition appears to mandate the population of health professional details, which it seems could only be the author of a completed assessment report which won't always exist. To help aid understanding and facilitate assessment of the complexity involved, could the Authority please clarify whether the use of IF6 should be expected in the following example scenarios? 1) A referral is cancelled by DWP, e.g. because the claim has been withdrawn. 2) A paper-based review cannot be completed for a claimant who cannot be invited to attend a consultation. 3) A claimant fails to attend their consultation appointment. 4) Advice is given in respect of a claimant for whom there is no existing		

		assessment report. 5) Advice is given which does not change the recommendations given in the previous assessment report. 6) Advice is given which changes the recommendations given in the previous assessment report. 7) A rework referral is rejected as not meeting the defined rework criteria.		
67 (was 103)	Attachment 2.1 - Services Description 7.1.1.1 ServiceNow	Does DWP intend for the third-party suppliers using the new PIP application to log their incidents into ServiceNow? Will this be the same DWP Place (ServiceNow) system as the the one used by internal DWP staff?	Yes, the third-party suppliers will be onboarded to the DWP instance of Service Now (DWP Place), and yes, it is the same one used by internal DWP staff.	v8
68 (was 104)	Attachment 2.1 - Services Description 7.1.1.1 ServiceNow	Will there be a ServiceNow web portal interface for third party suppliers to enter their incidents relating to the PIP application, and to consult knowledge resources on the PIP application that the supplier of the application will provide?	Yes – third-party suppliers will be onboarded to the DWP instance of Service Now - DWP Place	v8
69 (was 105)	Attachment 2.1 - Services Description 7.1.1.1 ServiceNow	Is DWP's implementation of ServiceNow able to send automated emails to the application supplier?	Yes	v8
70 (was 106)	Attachment 2.1 - Services Description 7.1.1.1 ServiceNow	How will the application supplier be able to load the knowledge resources on to the DWP ServiceNow instance?	The third-party supplier will be onboarded to the DWP instance of Service Now - DWP Place, and this will enable them to upload the relevant knowledge articles	v8
71 (was 107)	Attachment 2.2 – Key Performance Indicators and Subsidiary	There is no definition (level) given for Minor / Serious / Severe KPI Failure. Can we assume that these failure levels do not apply and we should	Yes that is correct. If the 'Target Performance Level of 100% in 3	v8

	Performance Indicators Tables 1.5.1 Service Levels AHS KPI4 AHS KPI5 Severity Levels (5th column)	disregard the Service Points values given for them in the Service Points column?	hours' is not met then this will result in the 'KPI Service Threshold' being breached and the relevant service points will apply	
72 (was 108)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables 1.5.1 Service Levels AHS KPI6 Severity Levels (5th column)	There is no definition (level) given for Serious / Severe KPI Failure. Can we assume that these failure levels do not apply and we should disregard the Service Points values given for them in the Service Points column?	Yes that is correct. If the 'Target Performance Level' specified: 'All data lost from the PIP IT System is recovered within the applicable RPO timescales specified in RPO Strategy' is not met then this will result in the 'KPI Service Threshold' being met and the relevant service points will apply	v8
73 (was 109)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables 1.5.1 Service Levels SMS KPI3 Severity Levels (5th column)	There is no definition (level) given for Severe KPI Failure or KPI Service Threshold. Can we assume that this failure level and threshold do not apply and we should disregard the Service Points values given for them in the Service Points column?	Yes that is correct if the 'Severe KPI Threshold' is breached no higher service points will be applied Attachment 2.2 has been amended to split KPI3a and KPI3b	v8

97 (was 146)	Functional Questions	It is noted that the IF6 interface mandates the population of Health Professional ID, Name and Type, yet the Authority has confirmed in its response to CQ60 that IF6 is to sent in scenarios where there is no assessment report, and possibly even no health professional footprint on the referral at all. As a simple resolution to this, would the Authority be able to confirm that these fields within any IF6 message from PIP IT may be populated with dummy values in these fields, noting that in all cases the author of every clinical report will be clearly identified within the reports uploaded to the DWP's Document Repository Service?	The population of dummy values within the IF6 message would be acceptable in scenarios where there is no HP data associated with the referral as in the stated scenario(s).	v8
98 (was 155)	Regions	'The PIP ITT indicates that PIP IT is supported by IAS and Capita across 4 regions; Northern England and Scotland, Midlands & Wales, Southern England and Northern Ireland. As per our understanding, FAS service will be provided through 5 regions where the Southern England region is further divided into South East and South West. We also understand that the new suppliers need to setup and transition the FAS service between November 2022-July 2023 and both the new PIP IT Managed Services and FAS suppliers will start BAU operation from 1st August 2023. Will the authority confirm the PIP transition	That is correct. There potentially may be 5 different FAS Service Providers therefore that scenario will need planning for.	v8

		should be planned for the 5 regions with potentially 5 different FAS service providers?’		
170 (was 145)	SQL query	With reference to Section "9.6.4 All data is stored in SQL-based relational databases." Can the Authority provide the vendor(s) e.g. MS SQL Server, Oracle etc. of the SQL-based relational databases used by both Capita/IAS PIP IT Service?	IAS - Oracle Database Capita - Microsoft SQL Server	v12

02 Version 2
Attachment 17 Apper

Note: this embedded document in now included in Annex F to Attachment 2.1

ANNEX G – FUNCTIONAL REQUIREMENTS

035 Version 3
Attachment 20 - Q4.1

Table of clarifications

The following table details clarification questions raised during the further competition process with the Buyer's responses in the column headed "DWP Response", relevant to this Annex G. The provisions of this Annex G, and any related provisions in this Contract, shall be interpreted in accordance with the relevant DWP Response.

In this table, references to the "Authority" or "DWP" are references to the Buyer.

Question Number	Question Classification	Question	DWP Response	Published
26	Q4.1 Functional requirements	AQR_08 states that 'The solution must ensure that any assessment report selected for audit is saved in the DWP Document Storage System'. Reports selected for internal audit are not currently sent to DWP at all, other than when any internal audit has been completed and any required amendments made. DWP thus does not receive multiple version of the same report, other than in DWP-initiated circumstances such as rework and independent audit. Could the Buyer please elaborate on this requirement, covering for example: - at what point in the process such reports are to be sent to DRS (e.g. referral closure or earlier, at the point of selection)? - how any such draft reports are to be identified (e.g. 'draft' watermark, or no special identification)? - whether if sent at the point of selection and unchanged at audit, a further copy is required at the point of closure? - would the same apply to a PBR (PA3 report) which is retracted and replaced by a consultation (PA4 report)?	Reports will be sent to DWP at the point of selection for quality review and at point of closure. Reports sent to DWP at point of selection will be watermarked 'Quality Check' and date and time stamped. If report is unchanged a further version will be sent as the original will be watermarked 'Quality Check'. This process is for all types of reports selected for Quality Review.	v4

		- would the same apply to a PBR (PA3 report) which is retracted and replaced instead by an FTA outcome?		
28	Q4.1 Functional requirements	FEAP_01, FEAP_17 and Advice_28 all refer to FE received, covering aspects such as capturing it, printing it and sending it to the DWP Document Storage System. Could the Buyer please confirm that a textual description or transcription of that FE (e.g. as taken over the telephone, or received by email or received in hardcopy form) will suffice to meet these requirements? If not, could the Buyer please provide additional detail on what is required, particularly in relation to emails and hardcopy documents received by APs?	A textual description or transcription of the Further Evidence is acceptable where a hard copy is not available. Hard copy Further Evidence should be forwarded to DWP Document Storage Solution.	v4
29	Q4.1 Functional requirements	Enq_11 refers to the creation of an email task when an email is received. Could the Buyer please confirm that the manual creation of a task within the solution by an AP user in response to an email being received within the APs' own systems (i.e. which are not integrated to the PIP IT solution) would suffice? If not, could the Buyer please provide more detail as to its requirements for integration of APs' own email solutions with the PIP IT solution?	A manual creation will suffice.	v4
30	Q4.1 Functional requirements	Enq_12 refers to the creation of a white mail task when white mail is received by the AP. Could the Buyer please confirm that the manual creation of a task within the solution by an AP user in response to white mail being received by APs (potentially within AP systems which are not integrated to the PIP IT solution) would suffice? If not, could the Buyer please provide more detail as to its requirements for any imaging of such white mail received, including provision of imaging facilities and integration with the PIP IT solution?	A manual creation will suffice.	v4

31	Q4.1 Functional requirements	ClExp_01, ClExp_02 and ClExp_03 refer to the capture and secure saving of claimant expense forms and receipts and the automatic creation of an expense record. It is noted that within (at least) Lot 1 and Lot 3 to date, expense claims and receipts have been processed by AP users without being imaged, and that requirement AM_56 indicates that expense claims will continue to be received on paper. In light of the Buyers evident intention to move away from the current approach, could the Buyer please provide more detail as to its requirements for any imaging of such expenses received, including provision of imaging facilities and integration with the PIP IT solution? Alternatively, if the current paper-based approach were to be acceptable, confirmation of this would be welcomed.	UPDATED in log v5 A clerical approach would be an acceptable solution. The Buyer has no requirements for any imagining of expenses received. CLExp_03 Requirement has been amended. CLExp_04 Requirement has been removed. Document 035 (Functional Requirements) and Document 01 (Instructions to Bidders - now Version3) have been amended to take account revisions detailed above and have been uploaded on Jaggaer	v4
42	Q4.1 Functional requirements	035 Attachment 20 - Q4.1 Functional Requirements - PIP IT Managed Service. (now Annex G to Attachment 2.1) Tab "FE Received" - Requirements FEDWP_01 to FEDWP_22 6 Unit Prices. The solution must ingest further evidence received details (FE) from PIPCS. Could you confirm if the scanned documents referenced in the FE received details are to be made available as part of the ingestion? If not could you clarify if access to view documents will be provided via API or via a DWP provided application on the EUD	FE received will be stored in the DWP Document Storage System and a task will be generated alerting the Provider that evidence has been received. The Provider will then be able to view this evidence via PIPCS. PIPCS will be accessed via an icon on the End User Device.	v5
61 (was 97)	Functional Questions	Functional requirement PA_11 states: 'The solution must generate a Return Assessment Function report when an assessment has been returned by this method.' It is understood that in the current business operation the Return Assessment Function is part of the PIPCS user	a) There are no scenarios where providers will interact with the PIPCS user interface as part of the referral closure process.	v7

		interface with which APs interact to return assessments in scenarios such as 1-5 above. Could the Authority please confirm: a) in what scenarios, if any, assessment providers will be expected to interact with the PIPCS user interface (i.e. as opposed to relying on IF6 automation) as part of the referral closure process? b) the type of information expected/required in the 'Return Assessment Function report'? c) whether the 'Return Assessment Function report' is a PDF to be uploaded into DWP's Document Storage Solution, or something else (e.g. data content to be passed through IF6)?	b) RAF types: Death, Failure to Attend, Failure to Comply, ID failure, Other, TI provision not met. Withdrawal, Failure to Comply, ID failure, Other require a justification to be recorded. c) A RAF report will be uploaded into the DWP Document Storage System. The RAF type will be sent to PIPCS.	
62 (was 98)	Functional Questions	Functional requirements ACT_145 and ACT_146 relate to the submission of incomplete assessment reports. Please could the Authority provide more information on this? It is believed that within at least two of the existing PIP lots, (as across the WCA operation), there are no scenarios in which a partial consultation report would be submitted to the Authority. There also appears not to be any reference to such a practice within the PIP Assessment Guide. If the underlying business need is simply for evidence obtained during an abandoned consultation to be provided to the Authority, then this could be achieved in other ways than through an incomplete consultation report. Should the Authority explicitly require incomplete assessment reports to be provided, clarification would be helpful as to: - whether the incomplete report should be provided through the same mechanism as other completed reports (noting that validation in the current PIPCS closure screens would prevent this), or whether instead the 'Return Assessment File' function should be used; - whether such reports are expected to trigger potential internal audit selection and associated processes;	ACT_145 & 146 refer to the submission of an incomplete assessment report captured offline to be uploaded to online PIP IT (ACT_129) for BAU processing.	v7

		- if internal audit does apply, it would be useful to understand how such reports should be graded, in particular with regard to health professionals working towards gaining their approval from the Secretary of State (noting that the PIP Assessment Guide confirms the approval criteria to be 5 consecutive 'acceptable' reports); - if internal audit does not apply, it would be useful to understand the validity and standing of any such report authored by a health professional who is not yet approved by the Secretary of State, and whether the case manager would need to take that into account, and if so how they might be aware; - if a report was incomplete because a claimant became unwell, whether a 'claimant sent home unseen' appointment outcome should be recorded and the appointment rescheduled, and if so, whether the incomplete report from the earlier consultation should be provided to the Authority as well as the subsequent report which may well have been produced afresh by a different health professional.		
63 (was 100)	Functional Questions	In respect of preparation time and write-up time, functional requirements ACT_92 and ACT_95 state explicitly that 'the solution must allow the capture...in hours and minutes.' Given that it is understood that these values relate refers to periods of time rather than times of day, is the Authority able to confirm that user input in minutes alone (e.g., 60 minutes, 90 minutes etc.) would be acceptable?	The input of minutes alone would be acceptable.	v7
64 (new)	Functional Questions	Several functional requirements relate to the provision of information from Independent Audit (IA), e.g. IAR_03: 'The solution must inform the AP when a case has been selected for IA.' IAR_04: 'The solution must inform the AP of the outcome of the IA.' IAR_07: 'The solution must inform the AP when feedback has been captured at IA.'	The existing arrangements, as described would be regarded as fully meeting these functional requirements.	v7

		It is believed that APs are currently notified of IA feedback through clerical templates which IA send by secure email to APs. Accordingly, IA notifies the AP directly, rather than through any IT solution, when a case has been selected for IA, of the outcome of the IA, and when feedback has been captured at IA. Is the Authority able to confirm that the existing arrangements as described would be regarded as fully meeting these functional requirements, or whether a greater level of functional support for the process would be necessary? If the latter were the case, could the Authority please provide more detail in respect of those functional requirements?		
65 (was 99)	Functional Questions	Functional requirements ACT_64 to ACT_67 make reference to a specific selectable option of 'Not Obtained Consent' whereas, at least historically, clinical training, guidance and practice within lots 1 and 3 has covered three selectable options as below: - 'The claimant consented to a physical examination' - 'The claimant declined to consent to a physical examination' - 'No physical examination was necessary' Could the Authority please confirm whether mandating a selection from the above three options would be acceptable? At least historically, health professionals have been encouraged to provide case managers with as much relevant information as possible. It is still possible for the heath professional to capture pertinent observations even when a physical examination (that would require consent). ACT_66 would appear explicitly to prevent users from providing such information within 'examination free text fields'. Could the Authority please confirm its intent in this regard? ACT_66 to ACT_68 refer to examination free text fields but are not specific about which fields are. The term 'examination' is widely used to refer to the PA4 sections covering mental state, musculoskeletal overview and 'other systems', not all	Could the Authority please confirm whether mandating a selection from the above three options would be acceptable? 'No physical examination was necessary' is acceptable and can be manually input. The other 2 responses are intended to be covered in ACT_64 which allows the user to record whether or not consent has been granted. ACT_66: The Authority would expect that all pertinent observations are captured but would be recorded in the Informal Observations field. If consent was not obtained, then the physical examination free text fields would be populated	v7

		of which relate to a 'physical' examination for which consent would be relevant. Please could the Authority clarify this ambiguity? ACT_67 refers to the need to auto-populate fields with text 'to pass mandatory validation'. It seems that potential providers are thus required not only to build validation, but also to build functionality to work around that validation. Could the Authority please confirm its intent in this regard?	with 'Not obtained consent' as per ACT-67. ACT_66 to ACT_68: Functional examinations may cover one or more of: mental functioning, vision, cardiorespiratory system, musculoskeletal system as stated in the PIPAG. Consent is required for physical examinations but not the mental function examination. ACT_67: The intent of ACT_67 is to populate the physical examination fields when consent is not given to reduce the need for HP input. Please note ACT_123 refers to the validation of the assessment report - 'the solution must ensure that all mandatory 'fields' have been completed before an assessment is submitted as complete'.	
83 (was 119)	Functional questions	Functional requirements AM08, AM09, AM10 and AM11 all begin "The solution must create appointment slots..." It appears that AM08 and AM09 concern the creation of slots (i.e. available appointment times) into which appointments can then be booked, and that AM10 and AM11 concern the booking of appointments into such slots. For the avoidance of doubt, could the Authority please either confirm this or provide alternative clarification?	We can confirm that your interpretation is correct.	v8

84 (was 120)	Functional questions	Functional requirement AM_33 states 'The solution must send a "Short notice" appointment notification to the claimant, when the appointment is booked within 7 calendar days.' Please could the Authority provide more information on this? In particular, is the content/messaging within this notification expected to differ from notifications where the appointment was not booked at short notice? Could the Authority please also confirm (or otherwise) that appointments should not be booked for claimants without giving them statutory notice unless they have first agreed to waive their right to the statutory notice period?	There will be a difference in the content of the two notifications referred to. We can confirm that appointments should not be booked for claimants without giving them the statutory notice unless they have previously waived their right to the notice period.	v8
95 (was 144)	Functional Questions	The Authority has confirmed in its response to CQ55 that 'Approximately 50% of printed notifications are expected to require a Business Reply Envelope'. Could the Authority please confirm whether reply envelopes are to be included with claimant-facing notifications (e.g. to accompany claimant expense forms, which as per functional requirement AM_56 are to be sent with all Assessment Centre notifications)? Assuming this to be the case, then: - Could the Authority please confirm by whom these envelopes are to be provided (e.g. the Authority / each individual Assessment Provider / the one IT Managed Service Provider)? - Could the Authority please confirm that up to six different variants of return envelopes might need to be accommodated - i.e. a variant for FE requests addressed to DWP's mail opening unit, and up to five different assessment providers, each with its own individual return address? The question is asked because of the potential impact on the fulfilment process.	Business Reply Envelopes are to be sent to accompany the Claimant Expense forms as referenced in AM_56. Assessment Providers will supply the Business Reply Envelopes for responses which will be directed to themselves (ie. expense claims). DWP will provide the Business Reply Envelopes for the responses directed to DWP's Mail Opening Unit. . Your statement is correct, potentially 6 variants of reply envelopes will be required.	v8
96 (was 145)	Functional Questions	The Authority has confirmed in its response to CQ61 that 'there are no scenarios where providers will interact with the PIPCS user interface as part of the referral closure	An optimised solution with potential automation capability which minimises	v8

		process'. This suggests a vision of the 'closure process' becoming fully automated, i.e. with PIP IT both sending IF6 and uploading all requisite reports to the DWP Document Repository System. In light of this could the Authority please shed more light on the following functional requirements? - PA_03: The solution must allow a user to self-allocate closure tasks. - PA_01: the solution must allow manual allocation of closure tasks to other users. - PA_02: The solution must allow manual re-allocation of closure tasks from other users. - PA_04: The solution must allow access to a closure tasks by the allocated user. - PA_13: The solution must allow the user to confirm case closure. - PA14: The solution must complete claim closure upon confirmation. - PA_15: The solution must ensure that a user cannot be part of the closure process for an assessment they have submitted. - RAF_06: The solution must allow access to all outstanding (RAF) tasks. - RAF _07: The solution must allow the user to close all outstanding (RAF) tasks The question is asked because the above seem to depict the closure process as a human activity within a discrete process step.	the need for manual intervention would be acceptable, therefore the proposal would be compliant. The proposed solution must allow allocation / re-allocation / closure of tasks.	
173	035 Attachment 20 - Q4.1 (now Annex G to Attachment 2.1) Functional	There is a separation of requirements regarding the handling of FE Received from the DWP (FEDWP) and FE Received by the AP (FEAP). It is understood that the FE received from the DWP will be received via IF7 in the form of an FE Received task. The user is required to access PIPCS on the DWP EUD to view the relevant FE document	An FE document presented by the claimant should be posted to DWP MOU and relevant details recorded in the assessment report. When the FE is received by	v12

	Requirements - PIP IT Managed Service Requirements Section FEAP and FEDWP	in preparation for assessment. As regards the FE received by an AP, if an FE document is presented by the claimant at consultation is the expectation that the detail of the FE is textually recorded in the assessment report and the relevant document itself posted to the DWP for ingestion to PIPCS? An IF7 FE received task will then be received by the AP confirming receipt of the FE document and logged against the referral? If FE is received by an AP via an inbound communication from the claimant should the same approach be followed where an FE task is raised detailing the content of the communication but the FE document itself despatched to DWP for ingestion to PIPCS?	the MOU a task will be generated and sent to the Assessment Provider if the assessment is still with them. If an inbound communication (phone call) is received the details should be captured on PIP IT which will automatically generate a PDF containing the details to be stored as evidence on DRS in accordance with requirement PA_21.	

ATTACHMENT 2.2 – KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS TABLES

Table of clarifications

The following table details clarification questions raised during the further competition process with the Buyer's responses in the column headed "DWP Response", relevant to this Attachment 2.2. The provisions of this Attachment 2.2, and any related provisions in this Contract, shall be interpreted in accordance with the relevant DWP Response.

In this table, references to the "Authority" or "DWP" are references to the Buyer.

Question Number	Question Classification	Question	DWP Response	Published
14	Print types	KPI Section 1.3.1 Are there any delivery service pre-requisites (e.g. 1st Class, Special Delivery or Courier) and are there any specific print types that will use this service?	The standard is 1st Class and any variations to be agreed through change control process.	v3
76 (was 112)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables 1.6 Service Levels DSM KPI1 DSM KPI2 DSM KPI3 DSM KPI5 Resolution time Incident reduction	Do these KPIs measure incident resolution / volumes across all resolvers, i.e. resolution by DWP internal IT and any third party suppliers to DWP. If so, what is the impact if our performance is on target but the measurement is amber or red due to the actions of resolvers from other organisations?	These KPIs are the DWP standard and relate to all parties, both internal and external. There are no service credits associated with Red & Amber however all KPIs are reported to the DWP Digital Executive Team.	v8
77 (was 113)	Attachment 2.2 – Key Performance Indicators	SMS KPI3 states a target resolution time of 95% within 20 hours.	Yes SMS KPI 1,2 & 3 are measures of the PIP IT service with associated	v8

	and Subsidiary Performance Indicators Tables1.5 1.6 Service Levels SMS KPI1 SMS KPI2 SMS KPI3 DSM KPI1 Resolution Time	DSM KPI1 requires resolution within 1 Business Day regardless of priority. Do we assume that we are required to adhere to SMS KPI3 rather than DSM1? Similarly SMS KPI1 & SMS KPI2 require resolution times of less than 1 Business Day; again should we adhere to SMS KP1s 1 & 2 rather than DMS1?	service credits. DSM1 is for reporting purposes to the Digital Executive Team.	

78 (was 114)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables1.5 1.6 Service Levels SMS KPI1 DSM KPI2 DSM KPI3 Resolution Time	SMS KPI1 requires resolution for Severity 1 within 4 hours. DSM KPI2 & DSM KPI3 require resolution for Priority 1 90% within 2 hours. Do we adhere to SMS KPI1 rather than DSM KPI2 and DSM KPI3?	SMS KPI1 is a measure of the Severity of the Incident. DSM KPI2 & 3 are a measure of the Priority of the Incidents. There are no service points associated with the priority targets. The KPIs are reported to the DWP Digital Executive Team.	v8

79 (was 115)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables1.5 1.6 Service Levels SMS KPI2 DSM KPI2	SMS KPI2 requires resolution for Severity 2 within 8 hours. DMS KPI2 & DMS KPI3 require resolution for Priority 2 95% within 8 hours. Do we adhere to SMS KPI1 rather than DMS KPI2 and DMS KPI3?	SMS KPI2 is a measure of the Severity of the Incident. DSM KPI2 & 3 are a measure of the Priority of the Incidents. There are no service points associated with the priority targets. The KPIs are reported to the DWP Digital Executive Team.	v8

	DSM KPI3 Resolution Time			
81 (was 117)	Attachment 2.2 – Key Performance Indicators and Subsidiary Performance Indicators Tables1.5 1.6 Service Levels SMS KPI1 SMS KPI2 DSM KPI4 Service Provider Incident Resolution	DSM KPI4: "This KPI provides Service Providers with a view of their own individual performance". Will the Supplier be able to view this real-time within DWP's instance of ServiceNow? If not, how will we receive this view? The requirements for Priority 1 and Priority 2 are different from the requirements in SMS KPI1 & KPI2. Do we adhere to the SMS KPIs rather than the DSM KPIs?	For incidents there are reports based on DWP KPIs, and for problem management there are weekly and monthly reports – Suppliers can run these themselves from DWP Place.	v8
100	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	SLA measurement. When the DWP Service Desk triages an incident to the Supplier, does the SLA clock start at that point? i.e. there is no reduction in our agreed SLA resolution time as a result of delays at the DWP service desk or while the DWP service desk is attempting a first-line fix.	End to End (E2E) Incident Resolution SLA measures the time it takes from the point the incident starts to be logged (Open Time field on the Incident) to the point the resolver group advises the incident is resolved and sets it to “Resolved” state. The SLA measures time cumulatively so, if the incident has not been fixed, the SLA clock will recommence from the point the incident is taken out of Resolved state, and stop again when it is put back into Resolved. In summary, the SLA starts when the Incident is Live.	v9

101	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	SLA measurement. Does the ServiceNow clock stop while we are waiting for a response from DWP, the end user or other third party?	Yes, once the Incident is placed 'On Hold' the clock stops as awaiting user info for up to 5 days. If no response within 5 days 'DWP Service Now' will automatically place into 'In Progress' again and if no further info Incident should be places into 'Resolved'.	v9
102	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	We have sized our service management solution for the expected number of incidents based on the application and its required functionality. If volumes vary significantly from forecast, e.g. because of short-term peak in volumes, or a significant increase in user numbers, will relief be available for SLAs?	In such circumstances the Buyer will always provide prior notice and appropriate adjustments will be agreed with the Supplier.	v9
103	Schedule 2.2 Performance Levels. 6. Part B. Performance Monitoring. 3. Performance Verification	Performance Verification. If DWP tests on the system as a result of sending test messages cause degradation in service, will there be a relief for our SLAs?	In such circumstances the Buyer will always provide prior notice and appropriate adjustments will be agreed with the Supplier.	v9
104	Schedule 2.2 Performance Levels. 6. Part A. Performance Indicators and Service Credits. 2. Service Points	Will we be able to suspend or modify SLAs during Disaster Recovery?	Yes	v9

105	Schedule 2.2 Performance Levels. 6. Part A. Performance Indicators and Service Credits. 2. Service Points	Will there be relief for SLAs if issues arise as a result of Buyer or third party action or omission?	Yes	v9
138	Annex C. (Further Competition Questionnaire) to Attachment 4.1. 4.4 Non-Functional Requirements (Service Management Requirements) – 5%. 4.4n) Service Availability Notices	We assume that it will be possible to update Knowledge Base KB0022435 which holds all of the current Buyer IT systems availability in DWP Place by submitting a report showing a summary of our availability in line with the required KPIs. Can the Buyer confirm that this is correct?	Yes this is correct. We would expect the Supplier to update any knowledge as appropriate.	v10
188	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	114 The Buyer response to CQ 100 states that "the SLA starts when the Incident is Live". We assume that this means, for the Incident response KPIs, SMS KPI1, SMS KPI2, SMS KPI3A and SMS KPI3B, that if there is a delay before the Buyer First-Line service desk triages this to the Supplier, our time permitted to fix the issue will be the SLA minus the time spent by the Buyer's team on the ticket before we receive it (including for example any first time fix attempt by the Buyer service desk). We also assume that we will be entitled to SLA relief if this delay / reduced time causes an SLA breach, e.g. we only have 3.25 hours to fix a Severity 1 incident instead of the stated 4 hour SLA, but we actually do fix it within 4 hours. Can the Buyer confirm these assumptions?	Your assumptions are correct	v13

189	Clarification Question - SLAs and Service Credits	We understand the SLAs and Service Credits which apply to the contract. Please can the Authority specify if the SLAs and Service Credits are applicable from	SLAs will apply from the (1) Operational Service Commencement Date	V13
201	SLAs and Service Credits	Thank you for your response, please can you confirm when Service Credits will commence on 1st April or 1st August 2023.	SLAs will apply from the (1) Operational Service Commencement Date 1st April 2023	v13
208	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	125 SMS KPI3A Severity 3 and SMS KPI3B Severity 4 incidents have target performance levels of >= 95%. Where incident volumes are low, a single incident could account for more than 5% of total incidents, e.g. if there are 15 incidents in a service period, each incident accounts for 7%. We assume that where incident volumes are low, there will be an adjustment to this % value. Is this correct?	There is no adjustment for % value built into KPIs	v13
209	Attachment 2.2 - Key Performance Indicators and Subsidiary Performance Indicators Tables. 1.5 Service Management Services KPIs	126 SMS KPI3A Severity 3 and SMS KPI3B Severity 4 incidents are to be resolved during Operational Hours. We understand that most staff providing PIP assessment services work Mondays to Fridays. Are we correct in assuming that the clock for incident resolution includes weekends, so that for example a Severity 3 incident logged at 5:00 p.m. on a Friday needs to be resolved by 9:00 a.m. on the following Monday (20 hours)?	The clock for Incident Resolution is Priority 1/2 = 24x7x365 (366 in leap year), Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales so their assumption is incorrect	v14

The Key Performance Indicators (KPI) and Subsidiary Performance Indicators (SPI) that shall apply to the Operational Services are set out below:

KEY PERFORMANCE INDICATORS

1.1 KPI Reporting

1.1.1 The Supplier shall provide all Monthly reports, specified in this section, electronically to the Buyer by the 10th Working Day of the following month.

1.1.2 The Supplier shall report their performance against each of the KPIs and provide supporting data for each report as evidence.

1.1.3 The Supplier shall ensure that all reports are an accurate reflection of the Services performed during the relevant reporting month.

1.1.4 The Supplier shall agree with the Buyer the format of the KPI Report pack prior to the first set of reports being issued.

1.2 Application Hosting Services KPIs.

1.2.1 The following Key Performance Indicators shall apply to the Application Hosting Services in Attachment 2.1 Paragraph 4.

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
AHS KPI1	PIP IT Service Availability	Service Availability of the end to end PIP IT Service Measured 24x7 / 365 days per standard year OR 366 days per leap year This KPI will be broken down further into sub-KPIs for the constituent components of the system and agreed between the Supplier and the Buyer post contract award	Monthly	Target Performance Level: ≥ 99.9%	0	YES
				Minor KPI Failure: < 99.9% and ≥ 98.9%	1	
				Serious KPI Failure: < 98.9% and ≥ 97.9%	2	
				Severe KPI Failure: < 97.9% and ≥ 96.9%	3	
				KPI Service Threshold: < 96.9%	4	
AHS KPI2	Response Times Scaling Capability – UI Interaction	System Response Times	Monthly	Target Performance Level: ≥ 99.0% of 2.5 secs	0	YES
				Minor KPI Failure: < 99.0% and ≥ 98.0% of 2.5 secs	1	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				Serious KPI Failure: < 98.00% and ≥ 97.00% of 2.5 secs	2	
				Severe KPI Failure: < 97.00% and ≥ 96.00% of 2.5 secs	3	
				KPI Service Threshold: < 96.00% of 2.5 secs	4	
AHS KPI3	Response Times Scaling Capability - APIs	System Response Times	Monthly	Target Performance Level: ≥ >99.0% of < 50ms	0	YES
				Minor KPI Failure: < 99.0% and ≥ 98.0% of < 50ms	1	
				Serious KPI Failure: < 98.0% and ≥ 97.00% of < 50ms	2	
				Severe KPI Failure: < 97.0% and ≥ 96.0% of < 50ms	3	
				KPI Service Threshold: < 96.00% of < 50ms	4	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
AHS KPI4	Recovery Time Objective (RTO)	The Supplier shall recover the PIP IT System within the applicable RTO timescales	Monthly	Target Performance Level: PIP IT System recovered within 3 hours 100%	0	NO
				KPI Service Threshold: PIP IT System recovered within 3 hours 100%	4	
AHS KPI5	Recovery Point Objective (RPO)	The Supplier shall recover all data lost from the PIP IT System as defined in the RPO Strategy See Appendix C Qualitative Questionnaire Non-Functional Requirements – PIP IT Req Sec 4 – 4.2 e) Recovery Strategy (RTO)	Monthly	Target Performance Level: All data lost from the PIP IT System is recovered within the applicable RPO timescales specified in RPO Strategy	0	NO
				KPI Service Threshold: All data lost from the PIP IT System is recovered within the applicable RPO timescales specified in RPO Strategy	4	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
AHS KPI6	Access Management	The Supplier shall provide, remove or modify access (including password resets) in response to requests when appropriately approved, within 1 Working Day	Monthly	Target Performance Level: Access provided, removed or modified ≤1 Working Day of appropriately approved request	0	NO
				Minor KPI Failure: Access provided, removed or modified >1 Working Day and <2 Working Days of appropriately approved request	1	
				KPI Service Threshold: Access provided, removed or modified ≥2 Working Days of appropriately approved request	4	

1.3 Bulk Print Services KPIs

1.3.1 The following Key Performance Indicators shall apply to the Bulk Print Services in Attachment 2.1 Paragraph 5.

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
BPS KPI1	Print Despatch	The Supplier shall dispatch prints within 24 hours of print file being generated.	Monthly	Target Performance Level: ≥ 99.9% of prints dispatched within 24 hours of print file generation	0	NO
				Minor KPI Failure: < 99.9% and ≥ 99.8% of prints dispatched within 24 hours of print file generation	1	
				Serious KPI Failure: < 99.8% and ≥ 99.7% of prints dispatched within 24 hours of print file generation	2	
				Severe KPI Failure: < 99.7% and ≥ 99.5% of prints dispatched within 24 hours of print file generation	3	
				KPI Service Threshold: < 99.5% of prints dispatched within 24 hours of print file generation	4	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
BPS KPI2	Print Quality	The Supplier shall collate & handle print outputs correctly (i.e. contain the correct data and level of quality as defined by the configurable notification template).	Monthly	Target Performance Level: ≥ 99.9% of prints handled correctly	0	NO
				Minor KPI Failure: < 99.9% and ≥ 99.8% of prints handled correctly	1	
				Serious KPI Failure: < 99.8% and ≥ 99.7% of prints handled correctly	2	
				Severe KPI Failure: < 99.7% and ≥ 99.5% of prints handled correctly	3	
				KPI Service Threshold: < 99.5% of prints handled correctly	4	

1.4 SMS Notification Services KPIs

1.4.1 The following Key Performance Indicators shall apply to the SMS Notification Services in Attachment 2.1 Paragraph 6.

1.4.2 The Assessment Providers will be required to give a minimum 2 hours warning in the event of an assessment cancellation and the claimant will be informed of this short notice cancellation by a telephone call and SMS notification.

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
SNS KPI1	SMS Notification Despatch	The Supplier Solution shall deliver 100% of the SMS notification instructions to the Telecoms supplier for issue to the claimant's phone within 5 minutes of the SMS notification being raised by the Assessment Provider. Measurement is calculated for the period of the Operational Hours specified in Attachment 2.1 Paragraph 9.1.	Monthly	Target Performance Level: ≥ 99.9 % of SMS notification instructions received by Telecoms supplier within 5 minutes.	0	NO
				Minor KPI Failure: < 99.9% and ≥ 99.8% of SMS notification instructions received by Telecoms supplier within 5 minutes.	1	
				Serious KPI Failure: < 99.8% and ≥ 99.7% of SMS notification instructions received by Telecoms supplier within 5 minutes.	2	
				Severe KPI Failure: < 99.7% and ≥ 99.5% of SMS notification instructions received by Telecoms supplier within 5 minutes.	3	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				KPI Service Threshold: < 99.5% of SMS notification instructions received by Telecoms supplier within 5 minutes.	4	

1.5 Service Management Services KPIs

1.5.1 The following Key Performance Indicators shall apply to the Service Management Services in Attachment 2.1 Paragraph 7.

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
SMS KPI1	Severity 1 Service Incident resolution time	Number of Severity 1 Service Incidents for which the resolution time exceeds 4 hours See Schedule 2.2 Part II: Definitions – Section 4 Fix Times for definition of Severity	Monthly	Target Performance Level: All Severity 1 Service Incidents resolved within 4 hours	0	NO
				Minor KPI Failure: ≥1 and <2 Severity 1 Service Incident is not resolved within 4 hours	1	
				Serious KPI Failure: ≥2 and <3 Severity 1 Service Incidents are not resolved within 4 hours	2	
				Severe KPI Failure: ≥3 and ≤4 Severity 1 Service Incident are not resolved within 4 hours	3	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				KPI Service Threshold: ≥4 Severity 1 Service Incidents are not resolved within 4 hours	4	
SMS KPI2	Severity 2 Service Incident resolution time	Number of Severity 2 Service Incidents for which the resolution time exceeds 8 hours See Schedule 2.2 Part II: Definitions – Section 4 Fix Times for definition of Severity	Monthly	Target Performance Level: All Severity 2 Service Incidents resolved within 8 hours	0	NO
				Minor KPI Failure: ≥1 and <3 Severity 2 Service Incident is not resolved within 8 hours	1	
				Serious KPI Failure: ≥3 and <4 Severity 2 Service Incidents are not resolved within 8 hours	2	
				Severe KPI Failure: ≥4 and <5 Severity 1 Service Incident are not resolved within 8 hours	3	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				KPI Service Threshold: ≥ 5 Severity 2 Service Incidents are not resolved within 8 hours	4	
SMS KPI3A	Severity 3 Service Incident resolution time	Percentage of Severity 3 Service Incidents which were resolved within 20 hours and the percentage of Severity 3 Service Incidents which were resolved within 30 hours (counting only hours within the Core Hours) See Schedule 2.2 Part II: Definitions – Section 4 Fix Times for definition of Severity	Monthly	Target Performance Level: ≥ 95.0% within 20 hours	0	NO
				Minor KPI Failure: < 95.0% within 20 hours; ≥ 95.0% within 30 hours	1	
				Serious KPI Failure: < 95.0% within 30 hours	2	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
SMS KPI3B	Severity 4 Service Incident resolution time	Percentage of Severity 4 Service Incidents which were resolved within 30 hours and the percentage of Severity 4 Service Incidents which were resolved within 50 hours (counting only hours within the Core Hours) See Schedule 2.2 Part II: Definitions – Section 4 Fix Times for definition of Severity	Monthly	Target Performance Level: ≥ 95.0% within 30 hours	0	NO
SMS KPI4	Problem Resolution Time	Number of Problems in the month which were not resolved in the time specified by the Problem Board	Monthly	Target Performance Level: All Problems specified by the Problem Board to be resolved in the month were resolved by the date specified by the Problem Board	0	NO

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				Minor KPI Failure: Only one Problem specified by the Problem Board to be resolved in the month was not resolved by the date specified by the Problem Board	1	
				Serious KPI Failure: Two Problems specified by the Problem Board to be resolved in the month were not resolved by the dates specified by the Problem Board.	2	
				Severe KPI Failure: Three Problems specified by the Problem Board to be resolved in the month were not resolved by the dates specified by the Problem Board.	3	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
				KPI Service Threshold: Four or more Problems specified by the Problem Board to be resolved in the month were not resolved by the dates specified by the Problem Board.	4	
SMS KPI5	Complete, accurate and timely MI provision	Number of Business MI Reports due for delivery within that month which have not been delivered at the scheduled time	Monthly	Target Performance Level: All reports delivered at the scheduled time 100%	0	NO
SMS KPI6	Virtual Library Completeness	Notify Authority of documents uploaded into the Virtual Library See Paragraph Virtual Library of Schedule 8.4 – Reports and	Monthly	Target Performance Level: 100% within 24 hours	0	NO
				Minor KPI Failure: < 100.00 % to ≥ 99.5% within 24 hours	1	
				Serious KPI Failure: < 99.5% to ≥ 99.0% within 24 hours	2	

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
		Records Provisions		Severe KPI Failure: < 99.0% to ≥ 98.5% within 24 hours	3	
				KPI Service Threshold: < 98.5% within 24 hours	4	

1.6 Digital Service Management KPIs

1.6.1 Digital Service Management (DSM) KPIs are a consistent set of automated measures that are applied to all Incidents and Problems in DWP Place (Service Now). They are used to measure the performance of all Internal Service Provider (DWP) teams and are also applied to External Service Providers. KPI measures are reported in dashboards within the Performance Analytics module of DWP Place, with some also reported in Splunk dashboards, where data can be filtered by a number of different attributes, for example, Technical Service, Function and Service Provider teams.

1.6.2 The KPI Definitions are listed below in their entirety.

1.6.3 Incident KPIs

1.6.3.1 Currently 2 of the 5 measures - Incidents resolved in 1 Business Day and Incident Volume Reduction, are reported up to Digital Executive Team. The KPIs complement each other by measuring performance from different perspectives and priorities, including individual Service Provider teams, therefore providing an overall high-level view of “end to end” performance” and include:

- DSM KPI1 - Incidents Resolved in 1 Business Day.
- DSM KPI2 - E2E Incident Resolution (including Mean Time to Resolve)
- DSM KPI3 - E2E "Active" Incident Resolution
- DSM KPI4 - Service Provider Incident Resolution
- DSM KPI5 - Incident Volume Reduction

1.6.3.2 DSM KPI1 – Incidents Resolved in 1 Business Day

Description	This KPI provides a user experience view of Incident Resolution, measuring the time it takes from the point the incident is opened until the point the incident is resolved, regardless of where the incident is assigned and including all Incident states. All incidents, regardless of priority, are measured against the same target timescale of 1 Business Day.
Automated DWP Place measure	Yes
Measurement Start Point	The Incident Opened date/time
Measurement End Point	Measurement ends when the incident is set to Resolved Measurement recommences if the incident is reopened, i.e. set back to In Progress state after having been set to Resolved.
Target	Green: > 60% of Incidents resolved within 1 Business Day Amber: > 50% - ≤ 60% Red: < 50% The measure is also calculated against 3 Business Days and 5 Business Days, however these do not have any % achievement targets. For Priority 1 and 2, a Business Day equates to a 24 hour day, for Priority 3 and 4 it equates to a 10 hour day.
Measurement Hours	Priority 1/2 = 24x7x365 (366 in leap year) Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales

Data Scope	**In Scope** • Incidents closed in the reporting period. • All time that an incident spends in any state other than Resolved. **Out of scope** • No User Impact incidents (i.e. No User Impact tick box is checked), where there is no impact to the DWP customer and/or citizens. • Any time that an incident spends in Resolved state. • Any incident set to Cancelled state.
Additional Rule / Notes	It is possible that, if specific scenarios occur, an incident may take longer than a day (from the point the incident was raised) to be resolved, but still be recorded as being resolved within the 1 Business Day target, due to the way the KPI is calculated. ***Scenario 1 - Incident reopened after spending time in Resolved state*** A priority 4 incident initially takes 8 hrs to be resolved. It remains in Resolved state for 18 hrs waiting for the user to confirm closure, at which point the user advises that the fault has not been resolved fully. The incident is set back to "In Progress", with the resolving team fully resolving the issue after 1 hour. The time that is captured for the KPI is 9 hours (initial 8 hours plus further 1 hour) which is within the 10 hour target used to measure priority 3 and 4 incidents against a Business Day, and the incident is therefore marked as a pass. The overall time, however, is 27 hours. ***Scenario 2 – Incident priority is increased*** An incident is initially raised as a priority 4. After 12 hours the impact changes and it gets increased to a priority 2. The priority 2 measurement calculation starts from this point. The incident is then resolved after 13 hours. 13 hours is within the 24 hr target time used to measure Priority 1 and 2 incidents against a Business Day, and the incident is therefore marked as a pass. The overall time, however, is 25 hours. N.B. Scenario 2 could only occur where there is in an increase in priority. If the incident priority is decreased then the KPI measurement calculation retains the original start point of the Incident Opened time.

Measure Calculations	Performance achievement is aggregated for all incident priorities and is reported as a percentage $\frac{\text{Total No. Incidents closed in the reporting period resolved within target}}{\text{Total No. Incidents closed in the reporting period}} \times 100$
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.3.3 DSM KPI2 – E2E Incident Resolution (including Mean Time to Resolve)

Description	This KPI provides a user experience view of Incident Resolution, measuring the time it takes from the point the incident is opened until the point the incident is resolved, regardless of where the incident is assigned and including all incident states. Whereas Incidents reported under "Incidents resolved in 1 Business Day are all measured against the same 1 target, E2E Incident Resolution measures different Incident priorities against different target timescales. E2E Incident Resolution is measured as both a percentage achievement and an average/mean time (see Measurement Calculations section).
Automated DWP Place measure	Yes
Measurement Start Point	The Incident Opened date/time. Where there is an increase in incident priority, the measurement start point is the date/time at which the priority was increased (refer to Additional Rules/Notes section).
Measurement End Point	Measurement ends when the incident is set to Resolved. Measurement recommences if the incident is reworked, i.e. set back to In Progress state after having been set to Resolved
Target	Priority 1 = 90.00% in 2 hours Priority 2 = 95.00% in 8 hours Priority 3 = 95.00% in 20 hours (2 Working Days) Priority 4 = 90.00% in 30 hours (3 Working Days)
Measurement Hours	Priority 1/2 = 24x7x365 (366 in leap year) Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales

Data Scope	**In Scope** • Incidents closed in the reporting period. • All time that an incident spends in any state other than Resolved. **Out of scope** • No User Impact incidents (i.e. No User Impact tick box is checked), where there is no impact to the DWP customer and/or citizens. • Any time that an incident spends in Resolved state. • Any incident set to Cancelled state.
Additional Rule / Notes	<u>Priority increase</u> If the priority of an incident is increased, the clock starts again. The measure calculation only includes time from the point that the priority is increased and is measured against the higher priority. <u>Priority decrease</u> If the priority of an incident is decreased, the clock does not restart. The measure calculation retains its original Measurement Start Point, but all of the time is measured against the lower priority target.

Measure Calculations	Performance achievement is measured separately for each Incident priority and is reported as both a percentage and an average. **E2E Incident Resolution %** $\frac{\text{Total No. Incidents closed in the reporting period resolved within target}}{\text{Total No. Incidents closed in the reporting period}} \times 100$ **E2E Incident Resolution Mean Time to Resolve** $\frac{\text{Total time (hours) taken to resolve all incidents closed in the reporting period}}{\text{Total No. Incidents closed in the reporting period}}$
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.3.4 DSM KPI3 – E2E “Active” Incident Resolution

Description	This measure captures the time an incident spends assigned to any assignment group from the point the incident is opened to the point the incident is resolved, but only includes time spent in New, In Progress or On Hold-Awaiting Vendor incident states i.e. time when a resolver group should be actively trying to resolve the incident. The measure does not include any time where a resolver group may be waiting for further information from the user, or for confirmation from the user that the issue has been resolved. By measuring only the time an incident spent in an active state, this KPI assists in determining if an E2E Incident Resolution failure is attributable to the resolver groups, as opposed to the failure being due to the time an incident spent awaiting feedback from the user.
Automated DWP Place measure	Yes
Measurement Start Point	The Incident Opened date/time. Where there is an increase in incident priority, the measurement start point is the date/time at which the priority was increased (refer to Additional Rules/Notes section).
Measurement End Point	Measurement ends when the incident is set to Resolved. Measurement recommences if the incident is reworked, i.e. set back to In Progress state after having been set to Resolved
Target	Priority 1 = 90.00% in 2 hours Priority 2 = 95.00% in 8 hours Priority 3 = 95.00% in 20 hours (2 Working Days) Priority 4 = 90.00% in 30 hours (3 Working Days)

Measurement Hours	Priority 1/2 = 24x7x365 (366 in leap year) Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales
Data Scope	**In Scope** • Incidents closed in the reporting period. • All time that an incident spends in New, In Progress or On Hold-Awaiting Vendor states. **Out of scope** • No User Impact incidents (i.e. No User Impact tick box is checked), where there is no impact to the DWP customer and/or citizens. • Child Incidents. • Any time that an incident spends in On Hold-Awaiting User or Resolved states. • Any incident set to Cancelled state.
Additional Rule / Notes	Priority increase If the priority of an incident is increased, the clock starts again. The measure calculation only includes time from the point that the priority is increased and is measured against the higher priority. Priority decrease If the priority of an incident is decreased, the clock does not restart. The measure calculation retains its original Measurement Start Point, but all of the time is measured against the lower priority target
Measure Calculations	Performance achievement is measured separately for each Incident priority and is reported as a percentage $\frac{\text{Total No. Incidents closed in the reporting period resolved within target}}{\text{Total No. Incidents closed in the reporting period}} \times 100$
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.3.5 DSM KPI4 – Service Provider Incident Resolution

Description	An STP (Service Tower Provider) is an entity in DWP Place that 1 or more related assignment groups can be mapped to. Service Provider Incident Resolution (formerly "GSO" Incident Resolution) is reported against the Service Provider, defined by the STP in DWP Place, that resolved the incident, and measures the cumulative amount of time, in New, In Progress or On Hold-Awaiting Vendor incident states only, that the incident spent assigned to any assignment group mapped to that resolving Service Provider/STP. This KPI provides Service Providers with a view of their own individual performance and is particularly useful for those incidents that have been assigned to more than 1 Service Provider. Although Service Provider Resolution is reported against the resolving STP, it is also possible to measure performance for any Service Provider that an incident was assigned to.
Automated DWP Place measure	Yes
Measurement Start Point	The date/time that the incident is first assigned to a group mapped to the STP. Where there is an increase in incident priority, the measurement start point is either 1) the date/time at which the priority was increased (if assigned to the STP at that time), or 2) the date/time that the incident is next assigned to the STP after the priority increase has taken place, whichever happens sooner (refer to Measurement Hours section).
Measurement End Point	Measurement ends when the incident is set to Resolved. Measurement pauses if the incident is reassigned to a group mapped to a different STP and recommences if the incident is reassigned back to the STP in question. Measurement also recommences if the incident is reworked, i.e. set back to In Progress state after having been set to Resolved, and assigned back to the STP in question.

Target	Priority 1 = 90.00% in 2 hours Priority 2 = 95.00% in 8 hours Priority 3 = 95.00% in 20 hours (2 Working Days) Priority 4 = 90.00% in 30 hours (3 Working Days)
Measurement Hours	Priority 1/2 = 24x7x365 (366 in leap year) Priority 3/4 = 08:00 - 18:00 Monday to Friday, excluding public holidays in England and Wales
Data Scope	**In Scope** • Incidents closed in the reporting period that were resolved by the Service Provider. • All time that an incident spends in New, In Progress or On Hold-Awaiting Vendor states when assigned to the Service Provider. **Out of Scope** • No User Impact incidents (i.e. No User Impact tick box is checked), where there is no impact to the DWP customer and/or citizens. • Child Incidents. • Any time that an incident spends in On Hold-Awaiting User or Resolved states. • Any time that an incident spends assigned to an assignment group that is mapped to a different STP. • Any incident set to Cancelled state.

Additional Rule / Notes	Priority increase If the priority of an incident is increased, the clock starts again. The measure calculation only includes the time spent assigned to the STP from the point that the priority is increased and is measured against the higher priority. Priority decrease If the priority of an incident is decreased, the clock does not restart. The measure calculation includes all of the time spent assigned to the STP but is measured against the lower priority target.
Measure Calculations	Performance achievement is measured separately for each Incident priority and is reported as a percentage. Total No. Incidents closed in the reporting period resolved by the STP within target × 100 Total No. Incidents closed in the reporting period resolved by the STP
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.3.6 DSM KPI5 – Incident Volume Reduction

Description	Continue to drive the overall reduction of Incidents experienced by users on their Digital products by a minimum of 10% (on previous year's figures).
Automated DWP Place measure	Yes
Measurement Start Point	Not applicable.
Measurement End Point	Not applicable.
Target	10% Reduction in 19/20 totals vs 18/19 totals. Though an annual target, volume reduction will be monitored / reported monthly against the 10% target. Green: > 10% reduction Amber: > 5% - ≤ 10% reduction Red: < 5% reduction
Measurement Hours	Not applicable.

Data Scope	In Scope • Incidents raised in DWP Place during the reporting period. This includes both User Impacting ("no user impact" tick box is not checked) and Non-User Impacting ("no user impact" tick is checked) Incidents. Out of Scope • Any incident set to Cancelled state.
Additional Rule / Notes	
Measure Calculations	Performance achievement is aggregated for all incident priorities and is reported as a percentage. Baseline = Total number of incidents raised in previous year x100 Total number of user incidents raised in DWP Place Where the measure is reported monthly, or as a year to date figure, the baseline used is the total number of incidents raised for the same period the previous year.
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.4 Problem KPIs

1.6.4.1 The purpose of the Problem KPIs is to drive and reduce Problem Open to Fix Identified/Fix Implementation times and drive and increase Incident to Problem linkage. Average Problem Open to Fix Identified Time and Average Problem Open to Fix Implemented Time measures are reported up to Digital Executive Team and include:

- DSM KPI6 - Average Problem Open to Fix Identification Time
- DSM KPI7 - Average Problem Open to Fix Implementation Time
- DSM KPI8 - % Closed Incidents linked to Problems

1.6.4.2 DSM KPI6 – Average Problem Open to Fix Identification Time

Description	This KPI measures how long it takes for a Problem fix to be identified from the point that the Problem is opened. The purpose of the measure is to: • Drive and reduce the time taken from a Problem being raised/opened to the Identification of a Fix; • Reduce disruption experienced by Users by preventing/reducing Incidents; and • Identify at a granular level specific Problems that are not progressing to the identification of a Fix i.e. are getting stuck in the earlier lifecycle phases and take appropriate action with the Problem Owner
Automated DWP Place measure	Yes
Measurement Start Point	The Problem Opened date In the event that a Problem requires more than 1 fix, for example if the initial fix is unsuccessful, It is likely that the Fix Identified position would remain the same as it was just the solution (implementation) that didn't work, However it is possible to go back to square 1 on the Problem and look for a completely different fix, in which case the Problem would be measured again from the original Problem opened date.
Measurement End Point	The date that the Problem is moved to Fix Identified stage. In the event that a Problem requires more than 1 fix, and a completely new fix is sought, then a new Fix Identified date would trigger, with the Problem being measured again up to the new Fix Identified date. If a completely new fix is not sought, then the original Fix Identified date is maintained and the Problem is not measured again.

Target	Using the 18/19 year 38-day average as a baseline, target/RAG status: Green: < 38 days Amber: > 38 - < 48 Red: > 48
Measurement Hours	Measured in days - 7 days a week, 365/366 days a year.
Data Scope	**In Scope** • All Problems recorded in DWP Place that are moved to Fix identified stage within the month being reported. **Out of Scope** • All other Problems that don't meet the In Scope criteria.
Additional Rule / Notes	Not applicable.

Measure Calculations	Performance is reported as an average, in days, using the following calculation: (A) Total No' of Problems moved to Fix Identified stage in DWP Place within the month being reported. (B) Total No' of days for the volumes in (A) to reach Fix Identified stage i.e. Opened date to Fix Identified date (C) Average Open to Fix Implemented time Calculation Formula - C = (B) divided by (A) Calculations take place immediately after the end of the month and therefore any Problems updated after the month end, for activities carried out during the month being reported, will not be included.
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.4.3 DSM KPI7 – Average Problem Open to Fix Implementation Time

Description	The KPI measures how long it takes for a Problem fix to be implemented from the point that the Problem is opened. The purpose of the measure is to: • Drive and reduce the time taken from a Problem being raised /opened to the Implementation of a Fix; • Reduce disruption experienced by Users by preventing/reducing Incidents; and • Identify at a granular level specific Problems that are not progressing to the implementation of a Fix i.e. are getting stuck in the earlier lifecycle phases and take appropriate action with the Problem owner
Automated DWP Place measure	Yes
Measurement Start Point	The Problem Opened date. In the event that a Problem requires more than 1 fix, for example if the initial fix is unsuccessful, then it is measured again, with each subsequent fix measured from the original Problem Opened date.
Measurement End Point	The Fix Implemented date If a Problem requires more than 1 fix, each subsequent fix is measured to the Fix Implemented Date for the specific fix in question.
Target	Using the 18/19 average of 128 days as a baseline, target/RAG status: Green: < 128 days Amber: > 128 - < 138 Red: > 138
Measurement Hours	Measured in days - 7 days a week, 365/366 days a year.

Data Scope	**In Scope** • All Problems recorded in DWP Place that have a Fix Implemented Date that falls within the reporting month. **Out of Scope** • All other Problems that don't meet the In Scope criteria.
Additional Rule / Notes	Not applicable.
Measure Calculations	Performance is reported as an average, in days, using the following calculation: (A) Total No' of Problems moved to Fix Implemented stage in DWP Place within the month being reported. (B) Total No' of days for the volumes in (A) to reach Fix Implemented stage i.e. Opened date to Fix Implemented date (C) Average Open to Fix Identification Time Calculation Formula - C = (B) divided by (A) Calculations take place immediately after the end of the month and therefore any Problems updated after the month end, for activities carried out during the month being reported, will not be included.
Reporting Source	Dashboards (DWP Place and/or Splunk)

1.6.4.4 DSM KPI8 – % Closed Incidents linked to Problems

Description	The KPI measures the percentage of Incidents, closed in the reported period, that are linked to a Problem. The purpose of the measure is to: • Drive and increase Incident to Problem linkage in order to provide visibility of, and fully understand, the impact on users caused by a Problem; • Drive analysis of those Incidents not Linked to Problems in order to identify Incidents trends/types and identify new Problems to be raised; and • Assist with accurate Problem prioritisation; ensure Problem fixes are effectively prioritised according to Business need. An incident is classed as being linked to a Problem if the Problem field in DWP Place is populated with a valid Problem number. Where an incident is not linked to a Problem, a mandatory field has to be completed and a reason provided.
Automated DWP Place measure	Yes
Measurement Start Point	Not applicable.
Measurement End Point	Not applicable.
Target	There is no achievement target associated with this KPI.
Measurement Hours	Not applicable.
Data Scope	**In Scope** • All incidents, including both user-raised and Proactively raised incidents, that were closed in the reporting period. • Any incident set to Cancelled state.

Additional Rule / Notes	Not applicable.
Measure Calculations	Performance is reported as a percentage achievement. Total No. Incidents closed in the reporting period that are linked to a Problem x100 Total No. Incidents closed in the reporting period
Reporting Source	Dashboards (DWP Place and/or Splunk)

2. SUBSIDIARY PERFORMANCE INDICATORS

2.1 SPI Reporting

2.1.1 The Supplier shall provide all Quarterly reports, specified in this section, electronically to the Buyer by the 10th Working Day of the following month after the quarter ends.

2.1.2 The Supplier shall report their performance against each of the SPIs and provide supporting data for each report as evidence.

2.1.3 The Supplier shall ensure that all reports are an accurate reflection of the Services performed during the relevant reporting quarter.

2.1.4 The Supplier shall agree with the Buyer the format of the SPI Report pack prior to the first set of reports being issued.

2.2 Social Value SPIs

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
SV KPI1	Social Value Tackling Economic Inequality MAC 2.2 MAC 3.2	• Number of full-time equivalent (FTE) employment opportunities created under the contract, by UK region. • Number of apprenticeship opportunities (Level 2, 3, and 4+) created or retained under the contract, by UK region. • Number of training opportunities (Level 2, 3, and 4+) created or retained under the contract, other than apprentices, by UK region. • Number of people-hours of learning interventions delivered under the contract, by UK region	Quarterly	• Good. The supplier is meeting or exceeding the SV KPI targets that are set out within the contract. • Approaching Target. The supplier is close to meeting the SV KPI targets that are set out within the contract. • Requires Improvement. The performance of the supplier is below that of the SV KPIs targets that are set out within the contract. • Inadequate. The performance of the supplier is significantly below that of the SV KPIs targets that are set out within the contract.	YES
SV KPI2	Social Value Fighting Climate Change	• Number of people-hours spent protecting and improving the environment under the contract, by UK region.	Annually	• Good. The supplier is meeting or exceeding the SV KPI targets that are set out within the contract.	YES

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information

	MAC 4.1	• Number of green spaces created under the contract, by UK region.
		• Annual:
		  • Reduction in emissions of greenhouse gases arising from the performance of the contract, measured in metric tonnes carbon dioxide equivalents (MTCDE).
		  • Reduction in water use arising from the performance of the contract, measured in litres.
		  • Reduction in waste to landfill arising from the performance of the contract, measured in metric tonnes.
				• Approaching Target. The supplier is close to meeting the SV KPI targets that are set out within the contract.
				• Requires Improvement. The performance of the supplier is below that of the SV KPIs targets that are set out within the contract.
				• Inadequate. The performance of the supplier is significantly below that of the SV KPIs targets that are set out within the contract.	

SV KPI3	Social Value Equal opportunity	• Total percentage of full-time equivalent (FTE) disabled people employed under the	Quarterly	• Good. The supplier is meeting or exceeding the SV KPI targets that are set out within the contract.	YES

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
	MAC 5.2 MAC 6.1	contract, as a proportion of the total FTE contract workforce, by UK region. • Number of full-time equivalent (FTE) disabled people employed under the contract, by UK region. • Total percentage of disabled people on apprenticeship schemes (Level 2, 3, and 4+) under the contract, as a proportion of the all people on apprenticeship schemes (Level 2, 3, and 4+) within the contract workforce, by UK region. • Number of disabled people on apprenticeship schemes (Level 2, 3, and 4+) under the contract, by UK region. • Total percentage of disabled people on		• Approaching Target. The supplier is close to meeting the SV KPI targets that are set out within the contract. • Requires Improvement. The performance of the supplier is below that of the SV KPIs targets that are set out within the contract. • Inadequate. The performance of the supplier is significantly below that of the SV KPIs targets that are set out within the contract.	

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
		other training schemes (Level 2, 3, and 4+) under the contract, as a proportion of the all people on other training schemes (Level 2, 3, and 4+) within the contract workforce, by UK region. • Number of disabled people on other training schemes (Level 2, 3, and 4+) under the contract, by UK region.			
SV KPI4	Social Value Wellbeing MAC 7.1 MAC 8.1	• Percentage of all companies in the supply chain under the contract to have implemented measures to improve the physical and mental health and wellbeing of employees. • Percentage of all companies in the supply chain under the contract to have implemented the 6 standards in the Mental	Annually	• Good. The supplier is meeting or exceeding the SV KPI targets that are set out within the contract. • Approaching Target. The supplier is close to meeting the SV KPI targets that are set out within the contract. • Requires Improvement. The performance of the supplier is below that of the SV KPIs targets that are set out within the contract. • Inadequate. The performance of the supplier is significantly below that of	YES

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
		Health at Work commitment. • Number of companies in the supply chain under the contract to have implemented the 6 standards in the Mental Health at Work commitment. • Percentage of all companies in the supply chain under the contract to have implemented the mental health enhanced standards, for companies with more than 500 employees, in Thriving at Work. • Number of companies in the supply chain under the contract to have implemented the mental health enhanced standards, for companies with more than 500 employees, in Thriving at Work.		the SV KPIs targets that are set out within the contract.	

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
		• Number of people-hours spent supporting local community integration, such as volunteering and other community-led initiatives, under the contract.			

2.3 Contract Management SPIs

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
CM KPI1	Contract Management Respond to the Buyer for any Call Off contract management matters	• Responding to correspondence (email or phone) from the Buyer within 2 Working Days • Resolving issues raised within 5 Working Days	Quarterly	Target Performance Level: =>95%	NO

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
CM KPI2	Contract Management Provide a report to detail the number of Call-Off Contract variations within each Quarter	Provision of the report 2 weeks after the end of each Quarter	Quarterly	Target Performance Level: =100%	NO
CM KPI3	Contract Management Management Charges to be paid within 30 calendar days from date of invoice issue	Confirmation of payment received by the Buyer within 30 calendar days	Quarterly	Target Performance Level: =100%	NO

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Publishable Performance Information
CM KPI4	Contract Management Provide accurate and full breakdown of pricing for Services within 14 Working Days of a request from the Buyer	Confirmation of receipt of full and accurate information by the Buyer	Quarterly	Target Performance Level: =100%	NO
CM KPI5	Contract Management Customer Service	% of responders who are satisfied or better at the end of SOW/ customer satisfaction report. The Buyer may use the Balanced Scorecard to score their satisfaction against Supplier's performance during that SOW.	Quarterly	Target Performance Level: =>90%	NO

ATTACHMENT 2.3 - ENVIRONMENTAL REQUIREMENTS

TABLE A – Prohibited Items

The following consumer single use plastics are Prohibited Items:	**Catering** • Single use sachets e.g. coffee pods, sauce sachets, milk sachets • Take away cutlery • Take away boxes and plates • Cups made wholly or partially of plastic • Straws • Stirrers • Water bottles
	Facilities • Single use containers e.g. hand soap, cleaning products • Wipes containing plastic
	Office Supplies • Plastic envelopes • Plastic wrapping for brochures • Paper or card which is bleached with chlorine
	Packaging • Single use plastic packaging from deliveries where avoidable e.g. shrink wrapped packaging from office supplier or facilities products. • Single use carrier bags
Buyer specific Prohibitions	*Not used*
Project specific Prohibitions	*Not used*

TABLE B – Permitted Items

Buyer Permitted Items	*Not used*
Project Specific Permitted Items	*Not used*

TABLE C – Sustainability Reports

Report Name	Content of Report	Frequency of Report
Sustainability Impact	a. the key sustainability impacts identified; b. sustainability improvements made; c. actions underway or planned to reduce sustainability impacts; d. contributions made to the Buyer's sustainability policies and objectives; e. sustainability policies, standards, targets and practices that have been adopted to reduce the environmental impact of the Supplier's operations and evidence of these being actively persued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; f. risks to the Service and Subcontractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks; and g. details of how the Supplier supports the Buyer's Green Government Commitment (GGC) Targets associated with greenhouse gas emissions, water consumption and waste production.	On the anniversary of the Effective Date
Waste created	By type of material the weight of waste categories by each means of disposal in the Waste Hierarchy with separate figures for disposal by incineration and landfill, including processes specific to the disposal of Waste Electrical and Electronic Equipment (WEEE).	Before Contract Award and on the anniversary of the Effective Date.

Waste permits	Copies of relevant permits and exemptions for waste, handling, storage and disposal.	Before the Effective Date, on the anniversary of the Effective Date and within ten (10) Working Days of there is any change or renewal to license or exemption to carry, store or dispose waste
Greenhouse Gas Emissions	Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in 'Greenhouse gas reporting – Conversion factors' available online at https://www.gov.uk/guidance/measuring-and-reporting-environmental-impacts-guidance-for-businesses	On the anniversary of the Effective Date
Water Use	Volume in metres cubed.	On the anniversary of the Effective Date
Energy Use	Separate energy consumption figures for: a. assets deployed on the Supplier's site; b. assets deployed off-site; and c. energy consumed by IT assets and by any cooling devices deployed. Power Usage Effectiveness (PUE) rating for each data centre/server room in accordance with ISO/IEC 31034-2/EN 50600-4-2.Confirmation that assets support the Buyer's Design Standards for Energy Use Intensity (EUI) Standards: • 70 kWhe/m2/year NLA at new offices • 115 kWhe/m2/year NLA at major refurbishments	On the anniversary of the Effective Date
Transport Use	a. miles travelled by staff when visiting the Buyer's sites from the Supplier's sites or home; b. resulting Green House Gas (GHG) emissions using agreed Conversion Factors; and c. the number of multi-lateral e-meetings i.e. with more than two attendees, held by type (audio,	On the anniversary of the Effective Date

	webinar, v/conferencing) their length and number of attendees.	
Materials	Materials usage, including: • type of material used; • quantity or volume of material used; and • amount of recycled/recovered material used.	Before Contract Award and on the anniversary of the Effective Date.

ATTACHMENT 2.4 - INFORMATION MANAGEMENT SYSTEM

Not Applicable

ATTACHMENT 3 - BUYER RESPONSIBILITIES

The Buyer shall, in relation to this Contract perform the Buyer's responsibilities identified as such in this Contract the details of which are set out below:

Document	Location (Paragraph)
Annex F to Attachment 2.1 (Appendix B Specification)	The Buyer will provide some support to the Supplier, for example providing help in understanding the governance steps required, acting as a subject matter expert on Personal Independence Payment and their systems.
Schedule 6.2	The Supplier must, therefore, consult and inform the Buyer, for example, the Buyer must witness any testing during development of the system. The Supplier must ensure regular reports / management information are available to enable the smooth implementation of the PIP IT Managed Service. Schedule 6.2 outlines the testing approach.
Annex F to Attachment 2.1 (Appendix B Specification)	Para 8.4: To support the PIP IT Managed Service rollout and provide the environment to move to HAS in the future the Buyer intends to provision the following: End User Devices (laptops & PCs) End User Environment (software and access to PIP IT Managed service) Networks to PIP sites Desktop based telephony (softphone) Local printing First line support for Assessment Providers
Extract from ITT submission 4.5c RAID log dependency tab	**Implementation & Migration** The Buyer will review and approve, within a reasonable period, all Deliverables and Milestones identified

Document	Location (Paragraph)
	in the Implementation and Migration plans
Extract from ITT submission 4.5c RAID log dependency tab	**Implementation & Migration** The Buyer will provide, in line with the timeline stated in the ITT, all resources and technology required to provide end user workplace services, including but not limited to 1LS Service Desk, end user devices, Active Directory, access to PIP CS, fileshares, and any DWP provided IT for all Assessment Providers.
Extract from ITT submission 4.5c RAID log dependency tab	**Implementation & Migration** The Buyer will provide a Zscaler proxy solution to enable secure end user access to the PIP IT services. This includes licensing for 5 Zscaler application connectors which will be utilised by the Atos solution
Extract from ITT submission 4.5c RAID log dependency tab	**Implementation & Migration** The Buyer will continue to provide existing WAN connectivity between DWP and Atos networks enabling connectivity to the Buyer's services
Extract from ITT submission 4.5c RAID log dependency tab	**Training** The Buyer will ensure that 1LS resources and trainers are available in line with the agreed schedule for technical and train the trainer training
Extract from ITT submission 4.5c RAID log dependency tab	**Training** The Buyer will deliver all training to Assessment provider and the Buyer's end users
Extract from ITT submission 4.5c RAID log dependency tab	**Implementation & Migration** The Buyer will define an overarching service model to which Atos will align for the delivery of an integrated service

ATTACHMENT 4.1 – SUPPLIER SOLUTION

In this Attachment 4.1, references to “Atos” are references to the Supplier.

Service Continuity with Fresh Thinking

4.1 Supplier Solution

Department for Work & Pensions

Atos

1. Supplier Solution

Supplier Solution Introduction

The five years between Operational Services Commencement Date of the Functional Assessment Services (FAS) IT Project and the rollout completion of the Health Assessment Service (HAS) being developed by the Buyer will be a period of innovation, disruption and change for all stakeholders, including the Health Professionals (HPs). We recognise that our role in this model will be to provide a safe pair of hands. We will run a national system that will provide the new FAS contract providers with consistent and reliable IT, enabling the Buyer to focus on enhancements to the overall process through the new HAS platform.

Atos carefully evaluated your ITT and considered a number of options to meet the Buyer's requirements. These included:

- Implementing new applications
- Re-writing our existing applications to make them suitable for native public cloud services
- Building on the existing applications we utilise to deliver PIP IT services today.

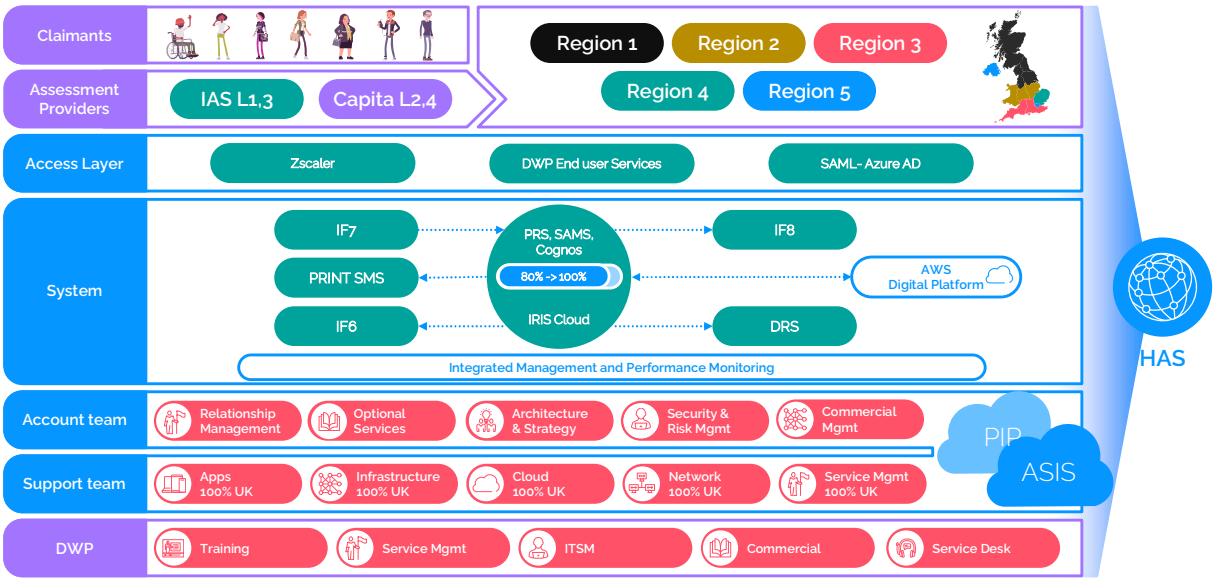
After a full evaluation we decided the best solution to meet the Buyer's requirements is to continue with the existing applications and augment the functionality to meet 100% of your requirements. There were three key drivers in our decision making:

1. The existing applications meet 80% of the Buyer's functional requirements with no modification, so limited change is needed to meet 100%
2. All of the current IAS assessment provider users (~70% of the FAS total) know the system so there is no disruption to their service
3. Building on the existing applications reduces complexity and risk

For these reasons Atos' solution will provide the Buyer with continuity and stability of the existing applications but also with enhancements to meet your new requirements.

Solution Overview

This solution overview outlines the key aspects of Atos' solution, which will be described in further detail throughout this document.



Claimants

Atos' solution will protect and enhance the claimant experience. We will provide stability of service, offer the least disruption approach, whilst making the FAS Assessment Providers more productive as we address your functional requirements.

FAS Assessment Providers

We believe our proposal will make your transition from IAS and Capita to the new FAS Assessment Provider model easier than anyone else. By the end of the implementation period the whole IAS team (representing ~70% of the Assessment Provider user base) will be fully trained and operational on an enhanced system meeting 100% of your requirements, so we can focus on the broader programme and integration with the new operating model.

Access Layer

The Atos solution will be fully integrated with the Buyer's new "cloud first" workplace environment and will be accessed via your Zscaler proxy service. Atos will support the Buyer to implement the ZScaler solution and will implement Z connectors in our platform to enable secure connectivity from your end user devices.

System

Atos' approach is to build on and enhance the proven system that we use today to deliver for IAS services. At the core of this system are three applications:

Patient Referral System (PRS): a proprietary case management application that has been continuously developed by Atos since 2013.

Siebel Appointment Management System (SAMS): a resource management and booking system built upon Siebel Appointment Booking application. SAMS has been modified by Atos to successfully underpin the IAS services.

Management Information Systems (MIS): Cognos management information and reporting applications providing insights into the data captured in PRS and SAMS

PRS, SAMS and MIS will continue to be hosted in **IRIS**, Atos' secure UK Government private cloud. IRIS provides a secure, scalable, highly available platform for the applications and is hosted in Atos' Birmingham Business Park (BBP) and Longbridge UK data centres.

We have chosen to continue with the existing solution because it meets 80% of your functional specification today so it offers the lowest risk transition to 100% of your requirements.

To supplement the existing applications and IRIS platform, Atos will also provide capability and expertise for future development on our AWS **Digital Platform**. The Digital Platform refers to Atos' public cloud hosted environment for secure enterprise consumption of AWS services. This platform has the potential to support the Buyer's development of the future HAS platform by showcasing our vision and capability to deliver fully cloud first, cloud native applications. Code from this Digital Platform can be used by the HAS team and ported into the HAS platform if the buyer wishes to do so.

The remaining 20% the Buyer's functional requirements which are not currently met will be assessed and, if appropriate, developed on this platform in line with Atos' drive to digitise customer systems and service operations. Where new functionality is not appropriate for the Digital Platform, Atos will fully meet the Buyer's requirements through enhancement to the existing PRS, SAMS and MIS applications.

Service and Performance Monitoring. The whole system is underpinned by Atos' secure management tooling platform, which provides 24*7 infrastructure monitoring and is integrated with Atos' ServiceNow for automated ticket generation. During the Implementation phase, Atos will extend the integration of our tooling into the Buyer's ServiceNow ITSM tool to ensure the Buyer has full visibility of the service.

We will also be implementing an Application Performance Management service to measure application response times and quickly identify the cause of service issues, enabling proactive service delivery for the Buyer and Assessment Providers.

Atos' Team

We will continue to utilise the existing UK based team that between them have decades of experience managing and developing systems supporting DWP assessment services. During the Implementation period there will be a thorough evaluation of the team, our processes and skills to ensure that any adjustments needed for the new service are made.

Our PIP IT team will work in an increasingly consistent way with our ASIS colleagues to ensure that the Buyer's programme learn the lessons from the ASIS programme. Atos went from providing a full assessment service, including IT, to providing IT services to Assessment Providers. We see many parallels with this programme and the journey that we are about to undertake with FAS.

The Buyer's Team

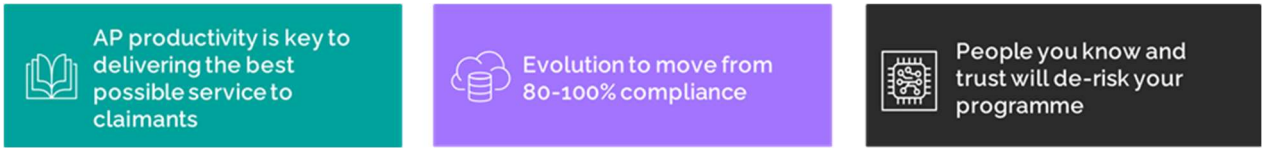
Atos recognises that we cannot deliver the services in isolation and ensuring that our services and processes are fully integrated with the Buyer's broader operating model is key. The service will be underpinned by the Buyer and the services you will provide to bring the whole claimant experience together. Atos will work collaboratively with the Buyer's team and Assessment Providers to collectively make the programme a success.

In summary, Atos' solution will provide stability and evolution, but with a fresh approach to service delivery.

2. Functional and Non-Functional Requirements

Functional Requirements

Atos has made the strategic decision to maintain and enhance the existing PIP IT system. This provides many benefits including of limiting the amount of development work needed to meet 100% of the Buyer's functional requirements.



Assessment Provider productivity.~70% of Assessment Provider users know our system so there will be no productivity dip as they learn a new system. We have been evolving this system since 2013 and introduced many features to improve Assessment Provider productivity, this programme will be continuation of that journey and will deliver maximum benefit to Assessment Providers at the earliest opportunity

Evolution from 80-100%. Atos solution meets 80% of the Buyer's functional specification today but that 80% includes some of the most complex functionality. There are some examples of complex developments Atos has built that only form small number of requirements, including auto booking appointments, risk-based audit rules engine and phrase builder. We believe that the remaining 20% is less complex and will be quicker to deliver. Our approach to delivery will mean that single work packages are able to address multiple areas of your requirements.

People delivering the programme. We believe we have earned the Buyer's trust through our deep-rooted skills and knowledge. The team that develops the functional solution will include people like Steve Heys and Jaideep Pillai who are intimate with our system and the Buyers assessment services.

Functional Requirement Gap Analysis

We have undertaken a comprehensive analysis to give the Buyer confidence that Atos' proposal represents the lowest risk. Some highlights from this analysis, picking out some areas where we have most work to do, are outlined in the diagram below.

Advice	86%
Appointment management	92%
Assessment completion tool	94%
Assessment quality review	85%
Change of circs	58%
Claimant expenses	73%
Complaints and RAR	86%
Enquiries	20%
FE received	59%
GP expenses	0%
Independent audit review	90%
Initial review	91%
IR quality review	100%
Management information	90%
Misc	61%
Post-assessment	82%
RAF submit incomplete	100%
Receive referral	83%
Rework	84%

Most of these gaps relate to the creation and allocation/ reallocation of tasks

Currently clerical

Includes multi-tenanting, and Welsh/ NI-specific requirements

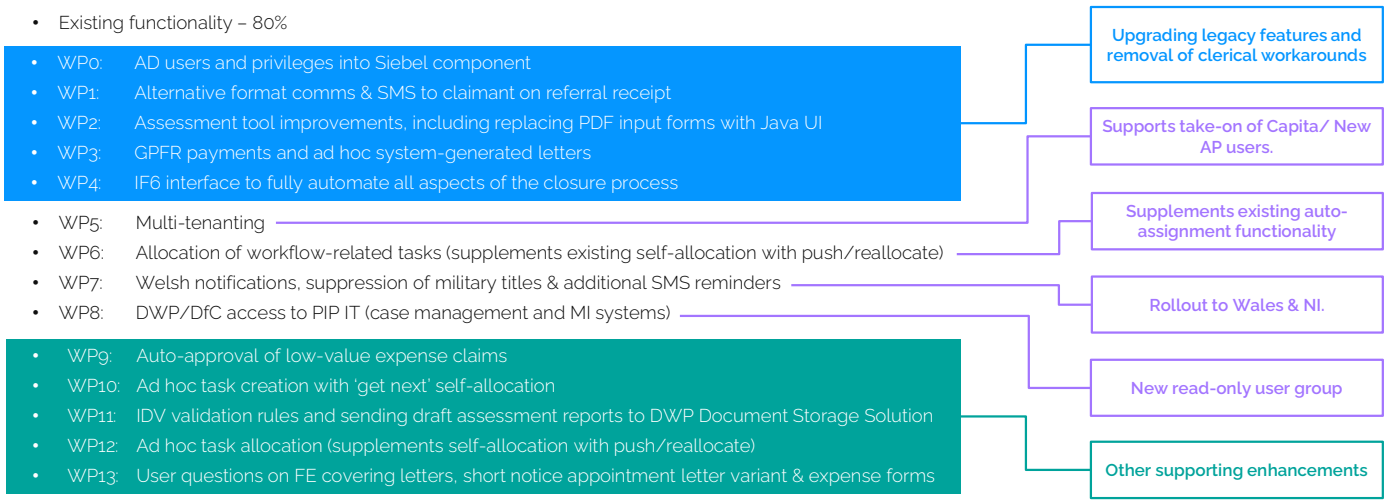
There are some areas where we currently do things differently, for example, GP expenses which is carried out off system today. Although we need to develop this functionality. The Atos team understand the business process and the related functionality so introducing this new requirement will be low risk.

Our approach means that many requirements are addressed by a small number of key features. Our programme will deliver features once and it will close gaps across multiple areas. For example, for *change of circumstances*, *enquiries* and *further evidence*, most of the requirements we need to achieve 100% in these areas relate to the creation and allocation/reallocation of tasks.

There are some key functions to enable new service such as multi-tenanting and Welsh notifications. Atos has already implemented similar features in MSRS and our organisational design for this programme will ensure the people with this experience are part of our team.

Delivering Functional Enhancements

Atos has designed 14 work packages to ensure our compliance with your functional specification moves from today's 80% to 100% during the Implementation phase. Each of these work package will address multiple requirements and have been sequenced so those delivering maximum benefit are developed early. This approach affords flexibility, so if the Buyer's priorities change Atos could on-board Capita users during the Implementation phase, allowing more time for the Buyer's broader programme. The diagram below outlines the work packages and the functionality each will deliver.



All of the work packages will be released incrementally to 70% of the Assessment Provider community so 100% will be in use and proven by IAS before the Viable Product Release. This means that there will be less end user training for the Buyer to deliver, allowing headspace for us collectively to focus on addressing the challenges that will inevitably occur in the broader programme.

We have a team of experts with the experience to deliver the functional solution. Many members of the team will be known to the Buyer as they have been instrumental in developing the existing PIP IT and MSRS before that, so between them have decades of experience in assessment services. We will also introduce experience of other successful programmes to ensure we balance knowledge of DWP PIP with implementation best practice.

Non-Functional Requirements

Atos will meet 100% of the non-functional requirements by by building on a foundation platform which is already 80% compliant today across the Compliance, Information and Service Management requirements.

We have undertaken analysis of the Buyer's non-functional requirements and identified the areas where enhancements are needed to achieve full compliance by either Viable Product Release or the Operational Service Commencement Date, dependent on when that requirement is needed. All of these enhancements are included in our Implementation and Migration plans.

Moving to 100% compliance for non-functional requirements

Atos will meet your non-functional requirements by utilising the existing sustainable platform with minimal change, ensuring that the appropriate enhancements are made to enable the functional requirements to be developed. PRS, SAMS and MIS will continue to be hosted in **IRIS**, Atos' secure UK Government private cloud. IRIS provides a secure, scalable, highly available platform for the applications and is hosted in Atos' Birmingham Business Park (BBP) and Longbridge UK data centres.

We have chosen to continue with the existing solution because it meets 80% of your requirements today so it offers the lowest risk transition to 100% of your requirements.

Sustain and support increase in productivity

- Tried and trusted platform.
- Impact low – minimal disruption

We will meet 100% of requirements

- Our Infrastructure as a service is ready to run
- Use the foundation, build upon it
- Enhancements are scoped to address the remaining 20%.

Why this is the optimal solution for DWP

- Provides maximum head-start
- Far less disruption for your user base.
- No significant change to the current way of working, or application support process

Some of the key projects we will deliver to meet your non-functional specification include:

User access. Atos will support the Buyer to implement the ZScaler solution and will implement Z connectors in our platform to enable secure connectivity to your Zscaler solution. We have strong experience with this including successful delivery of a large scale ZScaler solution for connectivity across user groups all over the world for the BBC.

Scaling out the hosting platform. We will enable additional capacity on the IRIS platform to accommodate the additional application code required for the functional requirements, additional users and additional storage for Capita data which will be migrated into the platform. IRIS is easily scalable via a well-established service processes and there will be no interruption to current services as we do this.

Non-Functional Requirements – Service Management Model

Atos understands that a service management approach that is fully integrated with the Buyer and Assessment Providers is key to delivering the FAS service. We will become a support team, albeit a critical one, in the Buyer's broader service management model so making sure we have well established processes and touchpoints is critical. Atos will appoint an experienced Service Architect who will lead our team and jointly develop our operating model.

Sustain service levels – ensure a smooth transition

- Continue 100% with existing team
  - Zero loss of knowledge
  - Continual service quality

Enhance the service

- Implement Atos DPM
- Proactive
- Increase productivity

Continually improve

- Encouraging closer working with AS-IS service.
- Inject lessons learned "*We have been on this journey with you*".
- 'One Team' attitude to seamlessly move through FAS

Atos' Team. We will continue to utilise the existing UK based team that between them have decades of experience managing and developing systems supporting DWP assessment services. During the Implementation period there will be a thorough evaluation of the team, our processes and skills to ensure that any adjustments needed for the new service are made.

Our PIP IT team will work in an increasingly consistent way with our ASIS colleagues to ensure that the Buyer's programme learn the lessons from the ASIS programme. Atos went from providing a full assessment service, including IT, to providing IT.

Service Management Tooling. The whole system will continue to be underpinned by Atos' secure management tooling platform, which provides 24*7 infrastructure monitoring and is integrated with Atos' ServiceNow for automated ticket generation. During the Implementation phase, Atos will extend the integration of our tooling into the Buyer's ServiceNow ITSM tool to ensure the Buyer has full visibility of the service.

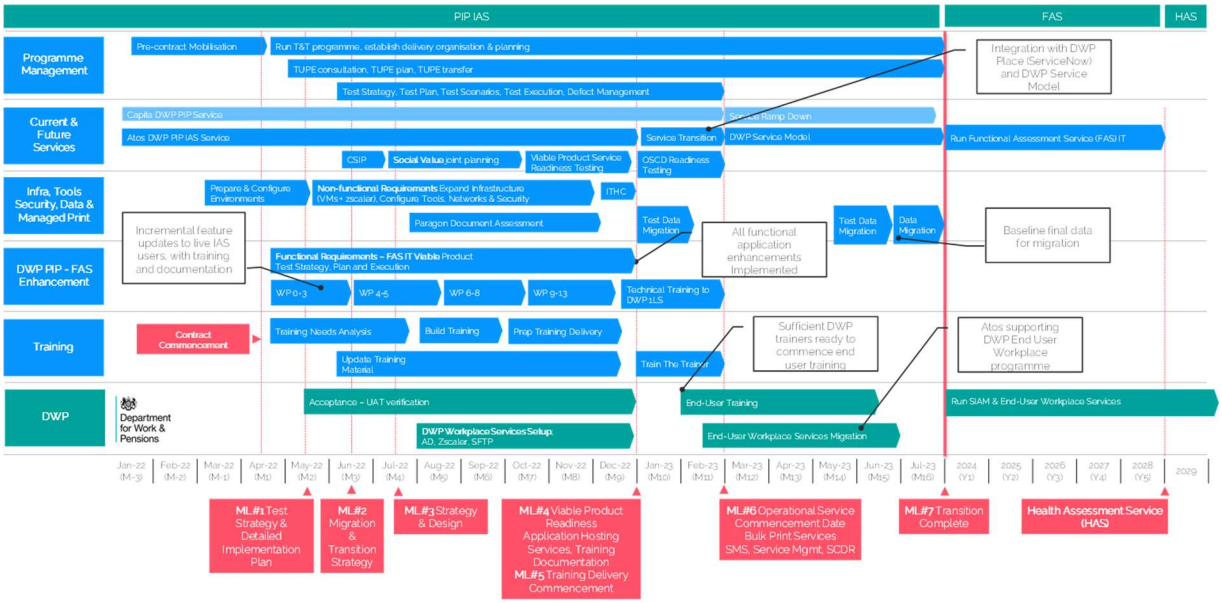
Application Performance Management. Atos is implementing Real Time Application Measurement, which will be supported by our Digital Performance Management (DPM) solution which drives efficiency by maximising the performance of the business-critical applications supporting our solution. The service collects relevant metrics for the solution landscape and sends them to the central platform. This central platform is underpinned by Dynatrace on which all monitoring, analysis and dashboarding will take place. This will provide Atos with a rich source of data to proactively manage the service and the Buyer will have an objective view of system performance to support the management of FAS suppliers.

3. Implementation, Migration and Transition Services

Overview

Atos will continue to utilise the existing PIP IT solution which meets ~80% of the Buyer's functional and non-functional requirements today and deliver a programme of enhancements to cover the remaining ~20% of requirements. We are in a privileged position to have this baseline solution, but we are not complacent, so our approach to Implementation will be rigorous to ensure we fully meet 100% of your requirements with the least possible disruption.

The Implementation, Migration and Transition overview diagram below shows our intended structure and plan to deliver the key products and milestones and provides as an overall view of implementation and migration. The diagram shows the workstreams running down the left-hand side against milestones running along the bottom.



This plan on a page is based on an extremely detailed project plan which has reached into each workstream across the organisation structure to extract the requirements, tasks, dependencies and risks, all of which are factored into our planning. The Atos plan will ensure that through joint working with the Buyer and Assessment Providers, we will achieve the critical completion milestone at the end of July 2023.

Implementation, Migration and Transition Organisation

The plan to deliver the functional and the non-functional enhancements will be managed and implemented by a skilled, experienced and integrated project organisation which is illustrated below. Many members of the team will be known to the Buyer as they have been instrumental in developing the existing PIP IT and MSRS before that, so between them have decades of experience in assessment services. We will also introduce experience of other successful programmes to ensure we balance knowledge of DWP PIP-IT with implementation, migration and transition best practice.

Implementation, Migration and Transition Organisation Chart
(Redacted FOIA S40(1) personal data)

[redacted]

Approach by Operational Service

The following table outlines our approach for Implementation, Migration & Transition for each of the Operational Services

Development Approach	Test approach	Migration & transition strategy	Service Management Strategy	Risk and issue management strategy
Applications Hosting Services				
Enhance existing applications used for DWP PIP IAS Increase IRIS hosting platform capacity Integrate with DWP workplace services Implement Application Performance Management (Response Measurement) solution Implement security tooling	Automated unit & integration testing Scripted UAT carried out by IAS Data migration test Perform ITHC	Incremental functionality released to IAS users Creation of training collateral Training DWP trainers	Creation of knowledge articles & Training of L1 support teams Audit of skills and certification for Atos support team Update to Service Design to reflect all latest platform and tooling information	Functional enhancements phased to offer maximum flexibility to Capita user migration Application access workaround available if DWP workplace plan changes Prioritise features which enable Capita users
Bulk Print Services				
Continuation of existing Paragon bulk print service Assessment of new/ changed print requirements against existing service Build new templates	Existing service but end to end integration testing undertaken by Atos/ Paragon Unit testing and overall system testing performed for revised volumes	Adjust print composition to meet new requirement Conduct initial testing prior to production changes, IAS users to perform production evaluation	Existing part of Atos integrated service Service management of Paragon service carried out by Atos seamless to DWP but visible to through Service Management	Existing service can be utilised to mitigate any risks identified

Development Approach	Test approach	Migration & transition strategy	Service Management Strategy	Risk and issue management strategy
			Services	
SMS Notifications Services				
Continuation of existing Paragon SMS. Assessment of new/ changed SMS requirements against existing service SMS System update /template build	Existing service but end to end integration testing undertaken by Atos/ Paragon Unit testing/overall system testing performed for revised volumes	Adjust SMS format to meet new requirement Conduct initial testing prior to production changes, IAS users to perform production evaluation	As per bulk print services Feed into Service Design	Existing service can be utilised to mitigate any risks identified
Service Management Services				
Integration of existing Atos tooling with DWP ITSM Alignment of ITIL processes with DWP service model New Service Design implemented New Service resources operational	End to end service process/tooling integration testing	Cutover to DWP service model at OSCD Atos will continue to progress existing tickets – no data migration Incremental feature release to IAS users in development plan	Align to Service Management Model	Service management integration brought forward to offer maximum flexibility to migration of Capita users Test features and training on IAS users in readiness for additional users

Development Approach	Test approach	Migration & transition strategy	Service Management Strategy	Risk and issue management strategy
Service Continuity and Disaster Recovery Services				
Inherent DR capability built into existing platform SC/ DR strategy incorporated during design/ development phase	SC/ DR testing undertaken during implementation	Ongoing SC/ DR services handed over to support during the migration period	Governance of SC/ DR testing agreed with DWP service management teams	Residual risks and issues identified during pre-migration testing will be managed via agreed risk management process
Optional Services				
Existing team/processes for delivery of optional services will be reviewed to identify and adjust require for new contract	Changes to services will be tested in line with DWP and the overarching service model	Cutover to new DWP service model at agreed OSCD date, controlled at stage gate review	Optional services will be handled in line with the revised DWP overarching service model	Optional services can be utilised ahead of OSCD as the vehicle to impact assess scope changes and expedite risk mitigation

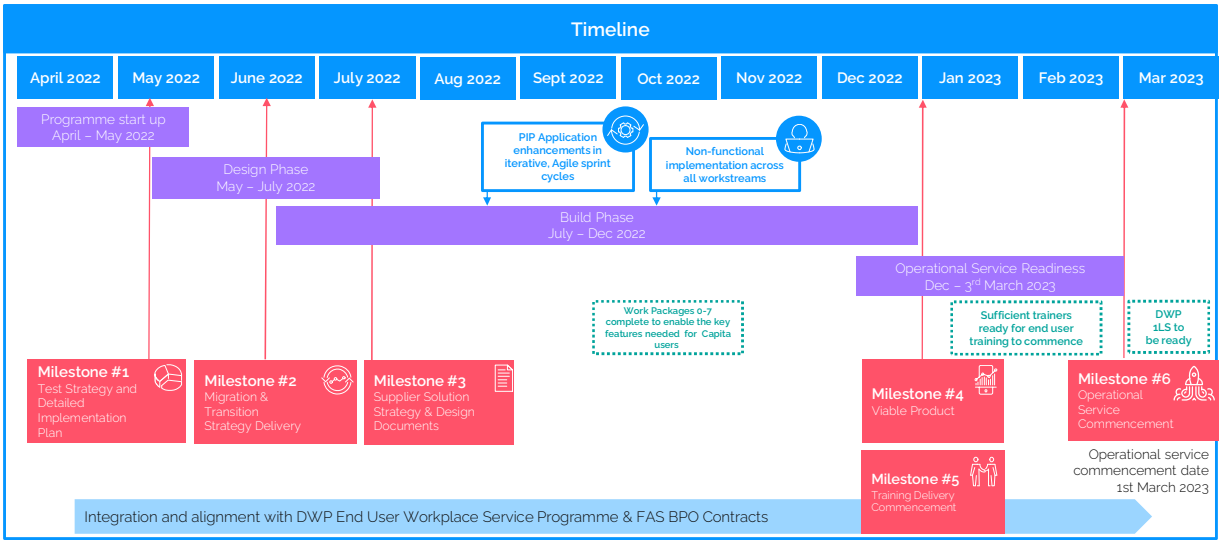
Implementation Plan

Our detailed MS Project (2016) implementation plan is included with our response. The plan covers the total scope and shows resource requirements and durations for each activity; it includes all tasks, milestones, deliverables and dependencies and Buyer responsibilities.

Our plan will form the basis for day-to-day control. It will be further developed and approved with input from the Buyer before commencing any work in relation to the implementation of the Services and will be updated and collectively assessed on a weekly basis.

To ensure success, the transition programme will align to the Buyer's governance model, and Atos will provide representation at the agreed meetings. It is expected the Implementation Plan will form a key input to the Programme Board meetings for downstream management of the transition.

The diagram below provides an overview of activities within Implementation which will take us to Operational Service Completion Date on 1st March 2023.The Implementation plan covers all functional and non-functional requirements and achieves all of the milestone dates running throughout implementation.



At the earliest opportunity we will jointly plan with the Buyer and Assessment providers to ensure it is aligned to the multiple programmes which need to be considered in parallel to this:

- DWP End User Workplace Services Migration programme
- FAS Assessment Provider contracts
- ASIS IT
- Any Exit Programmes within existing services.

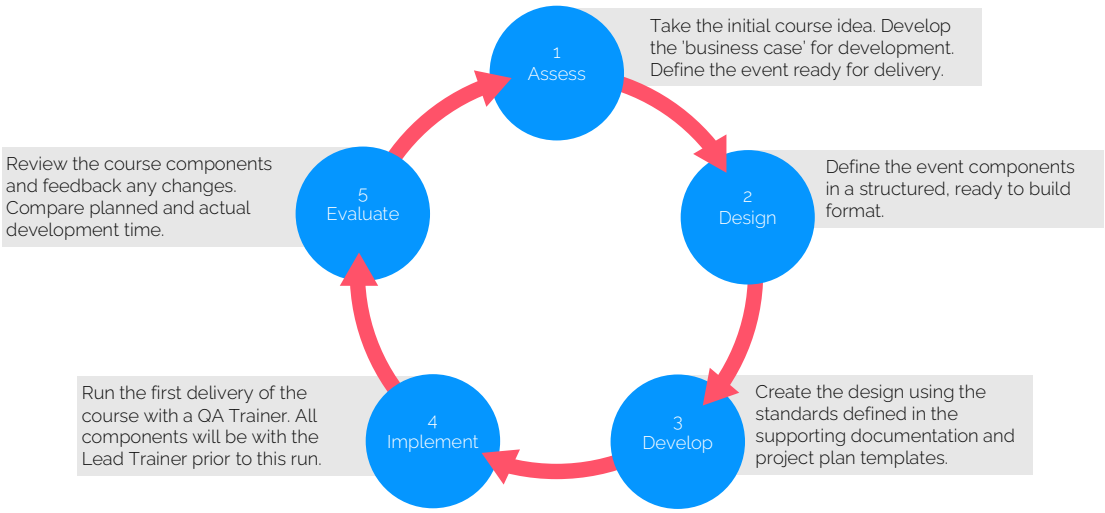
Our ability to support those interdependencies and our implementation approach and strategy will help align with these external programmes and ensure we enable the journey to FAS and ultimately to HAS.

During the Implementation phase we will introduce feature enhancements as soon as available, delivering value to live users and bring them a more feature rich product, enabling greater levels of productivity and ultimately an improved claimant experience.

Releasing features incrementally when developed also allows us test features with real IAS users, checking training material and feature capability and de-risking the later migration phase. It allows us to prepare service and operational teams to support new features, and to update training course information and documentation.

Provider Training

Atos has chosen to work with our proven training partner QA for development and delivery of training to the Buyer and Assessment Providers. QA have experience and multiple examples of delivering re-skilling/customisation and complex requirements for other government organisations, so they are familiar working in partnership with government departments. The diagram below outlines QA's training methodology:



Atos and QA will work with the Buyer to agree your preferred approach for approach for delivering train the trainer to your 250 trainers. The course will fulfil all of your requirements and will be relevant and motivational, and ultimately will enable these trainers to onward deliver their end user training to all users.

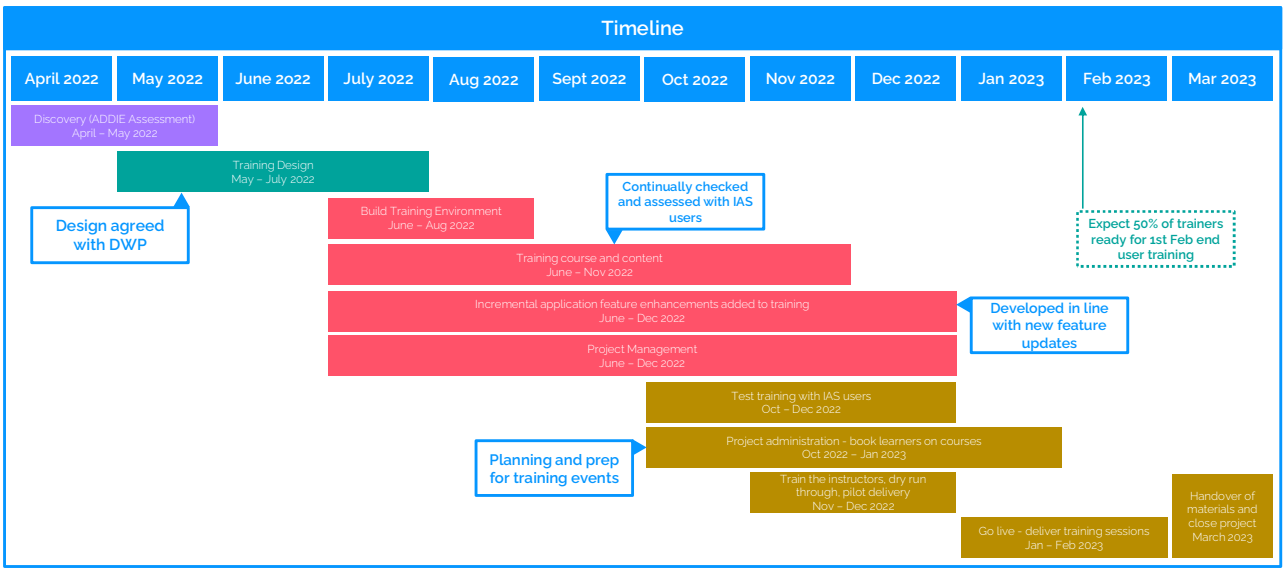
Our approach is flexible and we will be work with you throughout the process to ensure the training structure, materials and content are fit for purpose, considering online-live courses, training documentation and possibly face to face training, depending on the requirements agreed in the design phase.

All content will be broken down into a modular format as we recognise trainers will be having to deliver this training to a range of different PIP users with differing needs across the applications, so our solution will accommodate this.

We will ensure the 250 trainers are continually completing informal 'teach back' evaluation as a way of keeping the course interactive and engaging, but also completing a formal online assessment at the conclusion which demonstrates their overall understanding and expertise to be competent in onward delivering training on any part of the applications.

Training Roadmap

Our training plan considers the end-to-end development of training events and materials and based on our experience will be delivered in parallel with functional enhancements to the applications. The diagram below outlines the key activities and dates which we will jointly refine with the Buyer and Assessment Providers at the earliest opportunity.



Our plan means new features are built into training in parallel with their live release to IAS users, so the material remains up to date and relevant, but also considers how we can conduct testing of training and piloting materials on the existing IAS users. The IAS team will provide feedback and enable improvement, helping to validate what we're building is ultimately fit for purpose

We will be ready to commence train the trainer events from 1st January through to end of February and we've added some contingency into March to consider any changes or mop-up required. This means we'll have a sufficient number of the Buyer's trainers who will have completed their training by 1st Feb 2023 (we approximate possibly 50%).

With our approach, there will be early IAS training delivered by Atos, and less training overall as they know and use the applications already. The IAS team will be receiving training and information when the new features are built and deployed through the iterative development process. This means that the magnitude of user training needing to be delivered by the Buyer is significantly reduced, along with the risk.

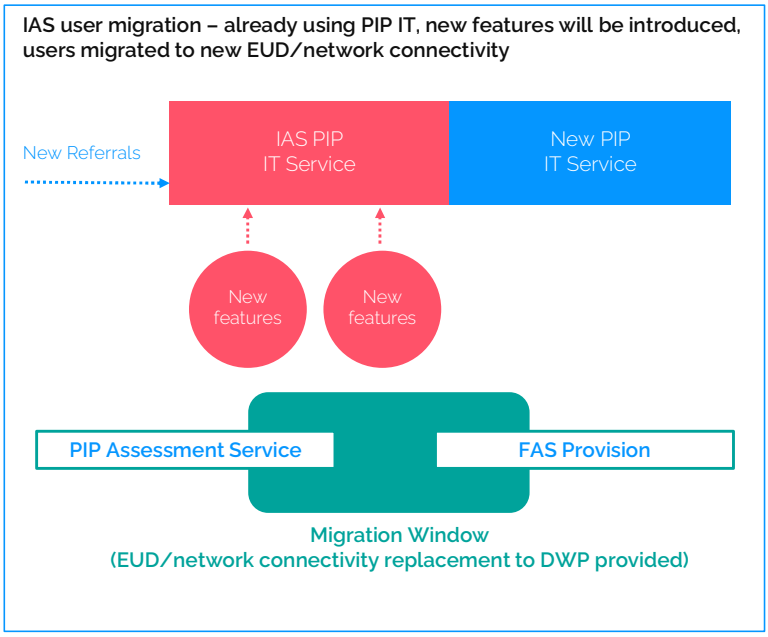
This plan and approach means we will work with the Buyer to focus on training Capita users on the system in readiness to allow for migration activities to progress. We will ensure the Buyer is ready to commence Capita end user training as soon as possible to de-risk the later stages of the Transition and enable early migration.

Migration Approach

Atos has designed two approaches for user migration, one for IAS users and another for Capita users. Th table below summarises the key activities required for each of the user groups and is described in further detail in the following sections.

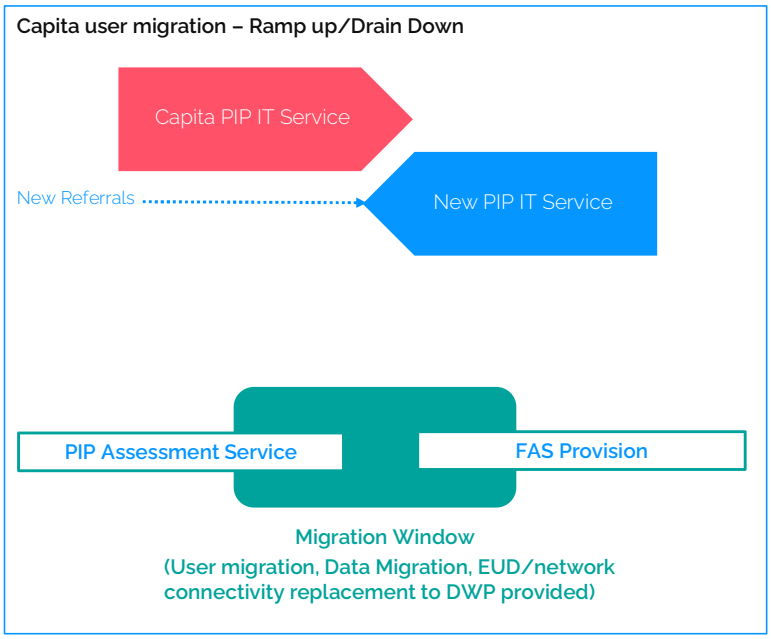
Migration Scope	IAS Users (70% of PIP)	Capita Users (30% of PIP)
Migration Design	✓	✓
Data Analysis	N/A	✓
Data Transformation	N/A	✓
Data Migration Testing	N/A	✓
Dress Rehearsal	N/A	✓
Data Migration (extract and load)	N/A	✓
End user migration to new PIP IT	N/A	✓

IAS Migration Strategy. As the Atos solution is to enhance the existing applications that the IAS team use today, there will be no migration to a new system needed for ~70% of the Assessment Provider user base. During the implementation phase, new functionality will be incrementally released to the IAS team so by the viable product date, all of the team will be utilising 100% of the functionality. The key activity for IAS during the Migration phase is migration on to the Buyer's new end user devices and infrastructure.



There will be no need for any data migration in respect of current lots 1 & 3, and all existing work will continue uninterrupted. The only changes for IAS users will be their connectivity method back to the current applications. This strategy allows the Buyer to undertake a controlled go-live for its new end user services and connectivity to the PIP IT solution and to prove it at scale before extending this to Capita users, all whilst allowing the current service to remain fully functional. This strategy allows for early testing of new feature releases, assessment of training, and completing the migration for this large user group early in the plan.

Capita Migration Strategy. Atos proposes a 'Ramp-up and drain down' migration approach for users serving the current lots 2 and 4. With this approach, some Capita users will remain assigned to the existing Capita solution to complete in-flight work, as others cutover to undertake new work on the PIP IT solution. The rate and geography of user transition should correspond with the rate and geography of ramp-up in respect of new referrals from PIPCS into PIP IT.



At an agreed migration start date, once Capita users have received training and service is ready, the new PIP IT solution will start to receive referrals for specific lot 2/lot 4 postcodes from PIPCS through IF7. These referrals will be processed entirely within the new PIP IT solution via the Buyer's new EUD and network connectivity by the first subset of Capita users to transition to PIP IT.

The proposed gradual switch-over of new referrals for Capita lots coming into PIP IT will see two distinct groups of users:

- Those awaiting transition, who continue to manage and complete existing referrals within their current Capita environment for the duration of the anticipated 12-week migration window, allowing for these to be closed within the current system
- Transitioned users, who now process new referrals using the new PIP IT solution using a Buyer provided laptop and Buyer connectivity.

At the end of the anticipated 12-week ramp up/drain down migration window, historical data (i.e. closed referrals) will be migrated from the Capita system to the new PIP IT solution in a one-off exercise, providing full visibility of this data within PIP IT. In the event of any outstanding cases remaining in the Capita system at the end of the migration window, Atos will work with the Buyer to agree a re-referral process to deal with these residual cases.

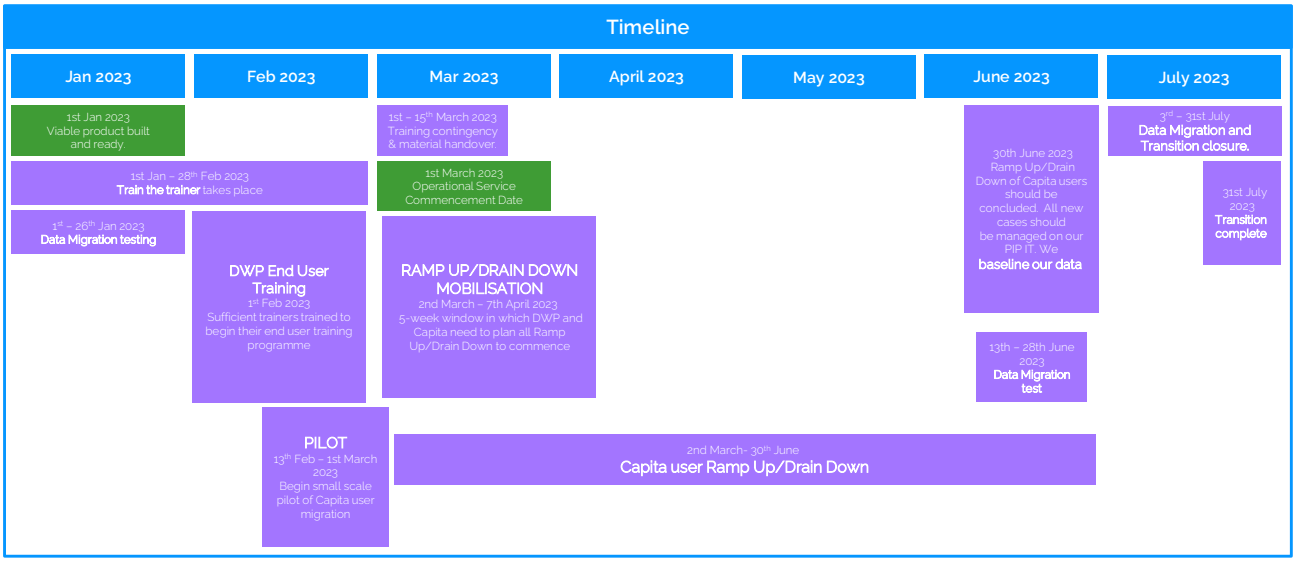
This migration approach aims to make the transition as risk free and straightforward as possible for the Buyer and Capita. The benefits of this migration approach to the Buyer and its users include:

- A clean cutover for individual Capita users, avoiding the complexities of individuals having to manage their workload concurrently across two separate non-integrated systems through different end user devices
- Avoiding double booking of resources (i.e., health professionals and appointment availability within consultation centres) across separate non-integrated systems

- Harnessing the geographical flexibility of telephone consultations to ensure continuity for claimants, as specific postcodes are migrated, affording the Buyer periods of assessment centre closure to accommodate any necessary network infrastructure upgrades.
- Avoidance of downtime of any PIP IT service
- Achieve key milestones of operational service commencement and transition completion in line with attachment 6.1.

Migration Timeline

Atos has developed a detailed Migration Plan, which is attached to our proposal, this diagram summarises the key activities and dates. The plan is built upon the products and milestones delivered in implementation that enable migration to commence safely (which you can see highlighted in green). Our migration plan is a proposal and requires joint planning with the Buyer and Assessment Providers to ensure deliverables from all parties are aligned.



Some key points from the plan:

- The key journey we consider within this plan is moving from end user training, enabling us to potentially target some small-scale pilot testing with Capita from 13th Feb 2023 for a 3-week window. This pilot will be supported by a Transition team
- In line with Operational Service Commencement Date, from 2nd March - 7th April is a critical 5-week window in which we collectively plan Ramp Up/Drain Down, so that every geographic region has started the approach no later than 7th April, which is the final cut off point to allow for 12-week drain down window before we baseline our data ready for migration.
- On 30th June we complete a final data baseline. This is the point in time where we want to have drained down Capita's system fully and have all cases being managed via our new PIP IT
- We've included a re-referral process within the planning in the event we do still have any live cases remaining on the Capita system at the end of their drain down window, to ensure these are moved across to the new PIP IT
- It's important to note we've captured risk mitigations within the plan , such as running multiple data migration tests prior to the final data migration. We have also built in contingency to the final data migration in the event of any issues
- Throughout July we will complete the Data Migration and will be moving to Transition Closure activities, meaning we achieve our ultimate milestone objective of a complete Transition on 31st July 2023.

4. Operational Services

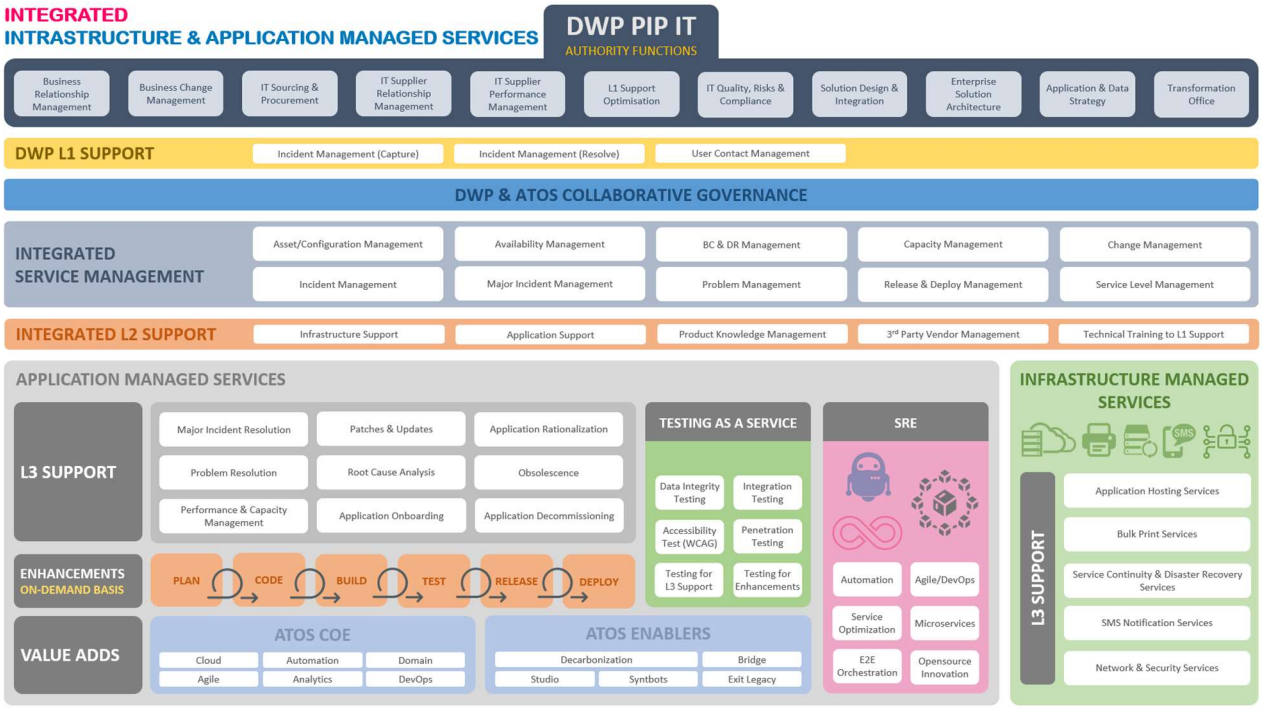
Service Management Services

To ensure continuity and zero loss of knowledge we will continue to utilise the existing UK based team that between them have decades of experience managing and developing systems supporting DWP assessment services. During the Implementation period there will be a thorough evaluation of the team, our processes and skills to ensure that any adjustments needed for the new service are made. This

Atos recognises that we cannot deliver the services in isolation and ensuring that our services and processes are fully integrated with the Buyer's broader operating model is key. The service will be underpinned by the Buyer and the services you will provide to bring the whole claimant experience together. Atos will work collaboratively with the Buyer's team and Assessment Providers to collectively deliver excellent services.

Target Operating Model

The Model below shows how our "Integrated Infrastructure & Application Managed Services (IAMS)" covers the functional and non-functional requirements with the other elements of the Buyer's functions and First Line Support.



Tooling

Atos' system is underpinned by our secure management tooling platform, which provides 24*7 infrastructure monitoring and is integrated with Atos' ServiceNow for automated ticket generation. During the Implementation phase, Atos will extend the integration of our tooling into the Buyer's ServiceNow ITSM tool, DWP Place, to ensure the Buyer has full visibility of the service.

To onboard the service operations to DWP Place, Atos will implement a Data Gateway integration between DWP Place and Atos' ServiceNow during the implementation phase to synchronise incident data between the systems. Incidents created and assigned in DWP Place by the Buyer's L1 support will reflect in Atos' ServiceNow for L2 or L3 support. Also, incidents generated in Atos' ServiceNow through system monitoring tools will reflect in DWP Place. Status updates made in incidents by L2 or L3 support will immediately reflect in DWP Place to enable L1 support track the incident for closure. Service Requests requiring attention by Atos L2 support will be manually managed in DWP Place.

We will also be implementing an Application Performance Management service to measure application response times and quickly identify the cause of service issues. Real Time Application Measurement will be supported by our Digital Performance Management (DPM) system which helps drive efficiency by maximising the performance of business-critical applications which support our solution. The service collects relevant metrics across the solution landscape and sends them to a central platform. This central platform is underpinned by Dynatrace on which all monitoring, analysis and dashboarding will take place enabling proactive service delivery. DPM integrates into ServiceNow so there is automatic proactive management, and quicker service response times without relying solely on the userbase to report incidents. The solution will provide objective data driven evidence to inform problem management and root cause analysis.

Application Hosting Services

Atos' approach for Application Hosting Services is to build on and enhance the proven system that we use today to deliver for IAS services. At the core of this system are three applications:

Patient Referral System (PRS): a proprietary case management application that has been continuously developed by Atos since 2013.

Siebel Appointment Management System (SAMS): a resource management and booking system built upon Siebel Appointment Booking application. SAMS has been modified by Atos to successfully underpin the IAS services.

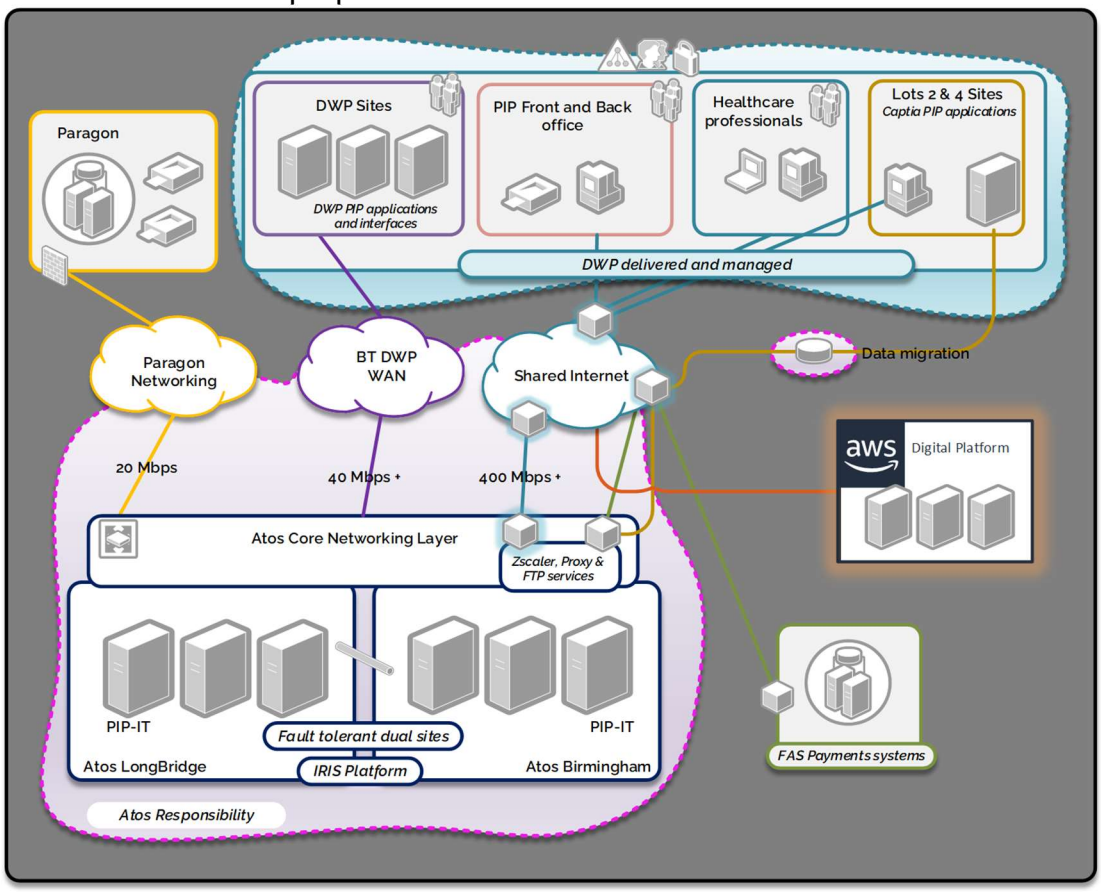
Management Information Systems (MIS): Cognos management information and reporting applications providing insights into the data captured in PRS and SAMS

Secure Hosting

PRS, SAMS and MIS will continue to be hosted in **IRIS**, Atos' secure UK Government private cloud. IRIS provides a secure, scalable, highly available platform for the applications and is hosted in Atos' Birmingham Business Park (BBP) and Longbridge UK data centres. We may, subject to full evaluation and agreement with the Buyer during the design phase, augment the existing hosting capability with an Atos managed AWS digital platform. Both platforms will be subject the same operational management processes and fully integrated toolset.

Network Connectivity

The DWP PIP WAN Circuit will remain in place to support connectivity from the Buyer to Atos hosted services. Atos will provide connectivity from the IRIS-hosted services to the Internet for access by the Buyer and Assessment Providers over a secure VPN tunnel. The diagram below illustrates the key components, the connectivity and interfaces within the proposed solution.



Federated Identity Management

Users will authenticate with the Buyer's Azure Active Directory via SAML to ensure an easy and secure entry into all PIP IT systems. SAML enables the communication between identity providers and service providers using secure tokens (encrypted, digitally signed XML-certificates) allowing users to access multiple applications with trusted information and using single sign on to only log in once. SAML removes user error (i.e., weak or forgotten passwords), improves user experience by not requiring credentials for multiple applications, and does so securely.

Security Services

Atos will continue to provide a series of robust security controls; Intrusion Detection and Prevention (IDP) using Fortinet technology, Secure File Transfer (SFTP) using Globalscape technology. Additional technologies will be provisioned during the Implementation phase; Internet Proxies for connectivity to DWP Place for the Zscaler infrastructure and Vulnerability Scanning Services (VSS) using Tripware technology. The Atos Client Security Manager is accountable for all security services and is a single point of contact for the Buyer for all security related matters. responsible for managing and tracking vulnerabilities for all components of the service.

Vulnerability Scanning. Atos will provide a vulnerability scanning service based on Tripwire to support our vulnerability management process. Standard vulnerability scanning enables Network host and Application discovery followed by identification, quantification, and reporting on vulnerabilities within the target environments.

Component Hardening. The IRIS Platform offers 'component hardening in line with CIS Benchmarks and is CHECK penetration tested as part of an annual ITHC. Other platform components including Networking, Storage and Compute equipment are hardened in line with vendor recommendations and/or CIS Standards and are subject to an annual CHECK penetration test.

Secure Coding. Atos follows "Security-by-Design" principles when designing software applications. Service designs are reviewed by experienced Security Architects to ensure; alignment to our design principles and by extension to the NCSC Security Design Principles, alignment to the Open Web Application Security Project (OWASP) Secure Coding Practices, use of secure protocols (including encryption settings), defence in depth, such that failure of a single component does not result in a major failure, segregations of duties, use of least privilege, thus protecting Personally Identifiable Information, secure configurations, compliance with Buyer's policies, i.e., cryptographic policy etc. Compliance metrics will be produced to evidence how the solution meets relevant guidance and "Security-by-Design" principles.

Security Patching. Security Patches are applied to the IRIS UK Platform in line with the Security Policy for Patching. This includes hardware firmware updates, BIOS updates, Operating System Patching and Management Tooling patching. All components of the IRIS Platform, both hardware and software, are lifecycle managed to ensure they remain in support with the vendor and subject to vendor security patching policies.

Penetration Testing Services. The IRIS UK Platform is subject to an annual CHECK Penetration Test and annual renewal of PSN Certification and Cyber Essentials Plus Certification.

Support team and processes

To deliver L2 & L3 Support services, Atos will form a dedicated, multi-skilled and experienced "Support Squad" with necessary technical skills (Java, etc.) that are required to support PRS, SAMS & MIS applications. This team will be made up of the existing team that have many years' experience managing DWP PIP IT applications and infrastructure and augmented with some fresh skills.

The setup will ensure hand-offs between the teams are seamlessly managed and maintains a culture of service ownership. Team 1 & 2 has an overlap of 5 hours to

ensure high volume of tickets are handled, and Team 3 overlaps with Team 2, so any outstanding tickets are transferred during non-operational hours. We have followed a similar approach with [redacted] Redacted FOIA S43 Commercial Interest This approach also supports the Buyer's "fix first" culture requirement to reduce its management overhead.

Added Value – Redacted FOIA S43 Commercial Interest [redacted]

Our "TaaS" (testing As a service) team will deliver all testing requirements such as Data Integrity Test, Accessibility Test (WCAG), Penetration Test and testing requirements from the L3 Support and Application Enhancements team.

The "Application Enhancement" team operates an "on-demand" basis to deliver projects in an Agile way. For International Olympic Committee, we have delivered 100+ Digital Transformation projects to transform legacy applications into cloud-native applications. We are experienced in many open-source development tools and methods and will package our capabilities within Buyer's "Application Enhancements" strategy to plan, forecast, and quickly deploy the backlogs with confidence to meet the business demands.

Our Support Squad will be using the expertise of our "Centre of Excellence (CoE)" team for any innovative ideas in the Cloud, Analytics, DevOps, Automation, Decarbonisation areas, and leverage our Exit Legacy tools for moving legacy applications to modern platform and technology; and tools such as Bridge, Syntbots, ThinkAI for Automation initiatives.

Service Continuity & Disaster Recovery Services

The service is hosted on IRIS which is designed for high availability with multiple levels of redundancy built into every layer ensuring no single point of failure, ensuring high availability. The solution is delivered from two tier 3 data centres in the Midlands region of the UK offering two availability zones enabling synchronous replication, high availability, business continuity and disaster recovery. The underlay network is built with N+1 Redundancy at every level. The core network is based on a Spine and Leaf Architecture with perimeter protection provided by four Next-Gen Firewall Clusters as displayed in the diagram below. The Inter-Site Dark Fibre Link is bonded fibre dedicated to Atos with diverse cable routes between sites and dual vendor DWDM multiplexers The diagram below provides a high-level view of Compute and Storage Redundancy

Twin Data Centre Compute & Storage Redundancy

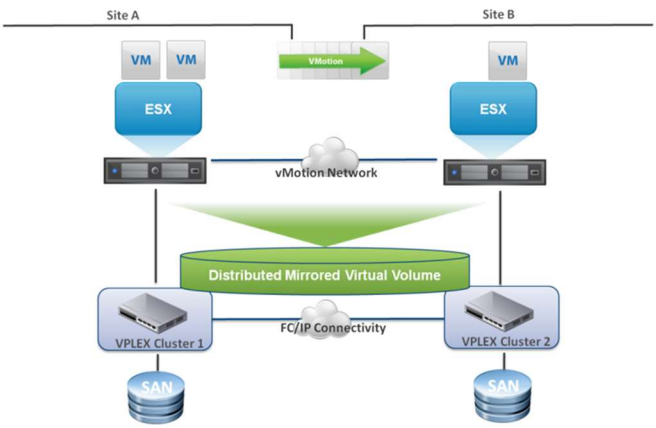
The IRIS UK Platform is hosted in two data centres within synchronous replication distance.

Independent physical networks with ability to span logical networks between sites with low latency.

Synchronous SAN storage replication with ability for simultaneous read/write at both data centres.

Latest VMware compute virtualisation software.

These technologies combine to create a virtual data centre that allows live migration of services between physical datacentres.



Atos has included a Service Continuity & Disaster Recovery (SCDR) Manager as part of our account team. The SCDR Manager is responsible for developing and maintaining SCDR plans which will be routinely tested in agreement with the Buyer and that Atos' PIP IT systems are compliant with RTO/ RPO KPIs.

Bulk Print & SMS Services

Atos will continue to provide bulk printing and SMS services with our existing supplier Paragon. In addition to the current DWP PIP Print and SMS services, Paragon provide similar services for other key Atos public sector clients including [redacted] Redacted FOIA S43 Commercial Interest. Paragon has the capability and scale to deal with the additional DWP PIP volume that is currently dealt with by Capita, they currently handle in excess of 6 billion mail items per annum.

Services provided under this sub-contract will include management & control of bulk print templates, performing bulk print runs & re-runs as necessary, provision of stationery & delivery of print outputs to the Buyers nominated mail delivery partner. For SMS Services this will include such services as the management and control of templates, updates to templates and issue of SMS notifications in accordance with dispatch deadlines.

All Paragon services are fully managed by Atos and will form part of the seamless integrated services we deliver into the Buyer.

5. Optional Services

Atos has included capabilities in our team to ensure we are able to respond to, develop and ultimately implement new and changed optional services for the Buyer. This activity will be led by our Customer Landscape Architect and CTO and will be operated utilising processes that we jointly agree with the Buyer ahead of OSCD.

Feasibility Assessments. We anticipate that potential new or changed requirements will be discussed by the Buyer and Atos at the Technical Review Board. From these initial discussions we will agree items to take forward for feasibility assessments. Atos will perform a high-level evaluation of the requirement to determine whether it is feasible to take forwards to a full requirements analysis phase, based in criteria to be agreed with the Buyer.

Requirements Analysis, Validation and Technical Options. Agreed requests will be taken forwards through a full requirements analysis process. Requirements will be drafted in an agreed format and analysed by Atos who will work closely with the Buyer for validation. Atos will prepare technical options for discussion with the Buyer at the Technical Review Board. Agreed options will be taken forward and Atos will create proposals for the Buyer's agreement in a format to be agreed ahead of OSCD.

Design Changes. Atos will design agreed changes in line with processes and in a format that is to be agreed with the Buyer ahead of OSCD. These changes will be reviewed and approved by the Technical Review Board.

Develop & Test Changes. Agreed changes will be developed and tested in an Atos development environment with regular validation from the Buyer that the changes continue to meet the agreed requirements. All changes under development will be included in the Atos programme for the Buyer.

Implementation and Release. Once changes have been fully tested and signed off by the Buyer, Atos will prepare for Implementation and Release. This activity will include preparation/ updates to documentation, training of technical support and the Buyer's 1LS on the changes as appropriate, training of the Buyer's trainers. Release of changes will always be carried out following the Buyer's change management process.

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/careers

Let's start a discussion together

Atos, the Atos logo, Atos Syntel, and Unify are registered trademarks of the Atos group. November 2021. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

ANNEX A TO ATTACHMENT 4.1: INFORMATION SECURITY QUESTIONNAIRE

Redacted FOIA S40(1) personal data

[redacted]

ANNEX B TO ATTACHMENT 4.1: DWP OFFSHORE PROPOSAL QUESTIONNAIRE

DWP Offshore Proposal Questionnaire

Redacted FOIA S43 Commercial Interest

[redacted]

[redacted]

[redacted]

[redacted]

ANNEX C TO ATTACHMENT 4.1: FURTHER COMPETITION QUESTIONNAIRE

Table of clarifications

The following table details clarification questions raised during the further competition process with the Buyer's responses in the column headed "DWP Response", relevant to this Annex C to Attachment 4.1. The provisions of this Annex C, and any related provisions in this Contract, shall be interpreted in accordance with the relevant DWP Response.

In this table, references to the "Authority" or "DWP" are references to the Buyer.

Question Number	Question Classification	Question	DWP Response	Published
44	Application and Data Segregation	In relation to question 4.2b can the Buyer provide further clarification on the application and data segregation in terms on types of data included in this requirement	In order to meet the requirements of the service the IT solution is expected to be multi-tenanted whereby all data will need to be segregated at Lot level and only allow access to FAS Assessment Provider users within the geographical lot of the claimant/referral. This will include but not be limited to the following data:- complaints, HCP, Appointments, Expense, Medical Outputs, Audit, Scheduling and capacity, Assessment Centre locations. There is no	v6

			requirement to restrict Authority user access within Lot structures	
185	4.3k Response Time Measurement	Question 4.3k refers to the Supplier's solution needing to 'enable response time measurements to be captured'. Can the Buyer please clarify whether the requirement is for the Supplier to provide a tool that measures and reports performance of the PIP applications (and if so where the measurement starts and stops), or that the Supplier's system needs to allow another system to collect data?	The Supplier needs to enable response time measurement within their own boundaries that supports the KPI/SLA obligations as detailed in Attachment 2.2	v13

Further Competition Questionnaire

1. **INTRODUCTION**

2.1 The Further Competition Questionnaire comprises of the following questions;

Compliance and Contractual Requirements – Pass / Fail – questions Section 3

Functional Requirements – questions Section 4.1

Non-Functional Requirements (Compliance Requirements) – questions Section 4.2

Non-Functional Requirements (Information Requirements) – questions Section 4.3

Non-Functional Requirements (Service Management Requirements) – questions Section 4.4

Management, Information and Support Requirements – questions Section 4.5

Social Value - questions Section 5

Pricing –questions Section 6

3.

1. Company Information

1	**COMPANY INFORMATION**	
1.1	**Please state your full company name**	**Atos IT Services UK Ltd**

2 Potential Provider Contact

2	**POTENTIAL PROVIDER CONTACT**	
2.1	**Please state the contact's name**	[redacted] Redacted FOIA S40(1) personal data

2.2	**Please state the contact's telephone number**	[redacted] Redacted FOIA S40(1) personal data
2.3	**Please state the contact's e-mail address**	[redacted] Redacted FOIA S40(1) personal data

3.1 Pass/Fail Questions

3.1a)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1a)	Off-shoring (including Landed Resources) In accordance with the DWP Offshoring Policy, prior written consent from the Buyer must be sought where Potential Provider's (and/or their sub-contractors) are proposing to host or access Buyer systems, services or official information outside of the United Kingdom, or to bring foreign nationals to the United Kingdom to provide services in delivery of the Contract. Potential Provider's must be aware of this and must submit an application for approval together with their tender. Where the Buyer gives consent, the Potential Provider shall comply with any reasonable instructions notified to it by the Buyer in relation to the Buyer Data in question. More information can be found in the document A Guide to DWP Offshoring Policy which can be found on Offshoring policy for DWP contractors - GOV.UK (www.gov.uk) DWP Offshoring Policy Buyer Data must not be processed outside the UK without the prior written consent of the Buyer and must at all times comply with the General Data Protection Regulation. The DWP Offshoring Policy controls apply when a contractor or sub-contractor wishes to: • Host DWP systems, services or official information outside the UK; • Allow staff based outside the UK to have access to DWP systems, services or official information; • Bring foreign nationals ("Landed Resources") to the UK to provide services including, but not limited to, applications development and support, testing and other similar activities. • Develop system applications outside the UK. • Send diagnostic data to an organisation outside the UK as a result of break/fix activity. Potential Provider's must respond Yes or No to this question and if the answer is yes then it must complete the DWP Off-shoring Proposal as part of its response to the ITT (included in Annex B to Attachment 4.1).	**Yes**	

3.1b)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer			
3.1b)	Freedom of Information Act 2000 The Authority is committed to open government and to meeting its legal responsibilities under the Freedom of Information Act 2000. All information submitted to the Authority may need to be disclosed by the Authority in response to a request under the Act. If you consider that any of the information included in your tender is commercially sensitive, please identify it and explain (in broad terms) what harm may result from disclosure if a request is received, and the time period applicable to that sensitivity in accordance with Contract Schedule 4.2. You should be aware that even where you have indicated that information is commercially sensitive, the Authority may be required to disclose it under the terms of the Act if a request is received. Please note that the receipt of material marked 'confidential' or equivalent by the Authority should not be taken to mean that the Authority accepts any duty of confidence by virtue of that marking. If a request is received, the Authority may also be required to disclose details to unsuccessful Tenderers. Potential Providers must respond Yes or No to this question and if the answer is yes then it must complete the Contract Attachment 4.2.	**Yes**	

3.1c)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1c)	Escrow Agreement Potential Providers are required to enter into an Escrow Agreement with the Authority and Escrow Agent; please confirm you will comply with this requirement.	**Yes**	

3.1d)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1d)	Information Security Questionnaire The Potential Provider must provide a completed Information Security Questionnaire (ISQ) in accordance with Contract Schedule 2.4 (included as Annex A to Attachment 4.1)	Yes	

3.1e)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1e)	Notified Key Sub-Contractors The Potential Provider must confirm by answering Yes or No to the question does your response involve the use of designated Notified Key Sub-Contractors. If yes, then the Potential Provider must complete details of Notified Key Sub-Contractors in accordance with Attachment 4.3.	Yes	

3.1f)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1f)	Software The Potential Provider must complete details of Software in accordance with Attachment 5.	Yes	

3.1g)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1g)	Supplier Project Plan The Potential Provider must confirm in writing that they have provided a Project Plan (MS Project 2016) in accordance with Management, Implementation and Support Requirements – question 4.5a in Appendix C in accordance with Contract Schedule 6.1	Yes	

3.1h)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1h)	Delivery timeline The Potential Provider must confirm by answering Yes or No to the question does your proposal meet the Authorities Key Milestone Dates in accordance with Attachment 6.1.	Yes	

3.1i)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1i)	Service Proposition The Potential Provider must confirm by answering Yes or No to the question does your delivery proposal meet the Services Description in accordance with Attachment 2.1	Yes	

3.1j)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1j)	Supplier Solution The Potential Provider must confirm in writing that they have provided a full description of the solution it is proposing for delivery of the Services by completing Contract Attachment 4.1 (Supplier Solution). The solution description to be provided in Contract Attachment 4.1 must: 1. Cover the Potential Provider's solution for: a. all Operational Services, as specified in Contract Attachment 2.1 (Services Description); b. all Optional Services, as specified in Contract Attachment 2.1 (Services Description). 2. Clearly demonstrate how (and which elements of) the proposed solution will deliver each of the individual Operational Services and Optional Services.	Yes	

3.1k)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1k)	Functional Requirements The Potential Provider must confirm by answering Yes or No to the question does your proposal meet the Functional Requirements in accordance with questions 4.1 of this Further Competition Questionnaire.	Yes	

3.1l)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1l)	Non Functional Requirements The Potential Provider must confirm by answering Yes or No to the question does your proposal meet the Non-functional Requirements in accordance with questions 4.2 to 4.4 of this Further Competition Questionnaire.	Yes	

3.1m) PASS/FAIL QUESTIONS		Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1m)	Pricing The Potential Provider must confirm by answering Yes or No to the question that you have provided a proposal that is fully priced in accordance with the pricing requirements of the ITT.	Yes	

3.1n) PASS/FAIL QUESTIONS		Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1n)	Alternatives / Variants The Potential Provider must confirm by answering Yes or No that they have not offered any alternative / variant solutions or options or funding models without the proposal being compliant with the specific requirements of the ITT.	Yes	

3.1o)	PASS/FAIL QUESTIONS		Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer. Potential Providers will not be disadvantaged where they are a new entrant to the market (trading for less than 12 months). In these circumstances the Potential Provider should confirm their commitment to achieving Net Zero by 2050 and should publish a full CRP as soon as possible.				
3.1o)	Carbon Reduction Plan (CRP) Net Zero The Potential Provider must confirm by answering Yes or No that you have detailed your environmental management measures by completing and publishing a Carbon Reduction Plan in accordance with the required Scopes and reporting standard set out in PPN 06/21 which must not have been completed more than 12 months prior to the date of commencement of the procurement. The Potential Provider must upload a link to your most recently published Carbon Reduction Plan in DWP e-PS system. In addition, Potential Providers should detail their current and baseline GHG emissions below. Marking Scheme: Not applicable as Potential Providers responses are for information only The provided emissions data will not be used as a basis for assessment in this Further Competition, but may be used to track Potential Provider's progress in reducing their emissions over time. https://www.gov.uk/government/publications/procurement-policy-note-0621-taking-account-of-carbon-reduction-plans-in-the-procurement-of-major-government-contracts		**Yes**	
	Baseline Year: 2018	Reporting Year: 2020		
	Scope 1: 30,383 tCO2	Scope 1: 11,920 tCO2		
	Scope 2: 63,675 tCO2	Scope 2: 50,660 tCO2		
	Scope 3: 128,078 tCO2	Scope 3: 86,420 tCO2		

3.1p)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer. Potential Providers will not be disadvantaged where they are a new entrant to the market (trading for less than 12 months). In these circumstances the Potential Provider should confirm their commitment to achieving Net Zero by 2050 and should publish a full CRP as soon as possible.			
3.1p)	Carbon Reduction (CRP) commitment Net Zero The Potential Provider must confirm by answering Yes or No that your organisation is taking steps to reduce your GHG Emissions over time and during the lifetime of this Further Competition and is publicly committed to achieving Net Zero by 2050. The Potential Provider must upload a link to your statement of commitment to achieving Net Zero by 2050 in DWP e-PS system: https://www.gov.uk/government/publications/procurement-policy-note-0621-taking-account-of-carbon-reduction-plans-in-the-procurement-of-major-government-contracts	Yes	

3.1q)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1q)	Declaration of compliance The Potential Provider must confirm by answering Yes or No that the Declaration of Compliance has been completed by a person with authority to act on behalf of the Potential Provider. This section also serves as a checkpoint for Potential Provider's to confirm that they have provided all the information required, including additional Attachments.	Yes	

3.1r)	PASS/FAIL QUESTIONS	Pass/Fail	
Please Note: The following question is a Compliance and Contractual Pass / Fail question, therefore if a Potential Provider cannot or is unwilling to answer 'Yes', their Tender will be deemed non-compliant and they will be unable to be considered for this requirement. The Potential Provider should confirm by deleting the inappropriate answer.			
3.1r)	Guarantee The Potential Provider must confirm by answering Yes or No that if they become the preferred supplier they will co-ordinate the signature of a Deed of Guarantee in accordance with Contract Schedule 10 where a subsidiary or demonstrate sufficient financial provision for Self Guarantee (if not a subsidiary).	**Yes**	

4 QUALITY Questions – 55%

4.1 Functional Requirements – 20%

The Functional Requirements of the ITT are contained within the Excel Spreadsheet Q4.1 Functional Requirements.xlsx in DWP e-PS. (Annex G to Attachment 2.1)

The Excel format used is due to the high volume of functional requirements against which Potential Suppliers are asked to respond. A Glossary of Terms is also contained within the spreadsheet. For each of the individual Functional Requirements there is a maximum word count of 100. Any information provided in excess of the 100-word count will be disregarded.

Please see the Further Competition Instructions to Bidders paragraph 22.16.1 for the Functional requirements detailed evaluation information including the marking scheme used for all of the individual questions in this section. Please note that each of the individual Functional Requirement questions have a pass mark of 66% associated with them. With a minimum total pass mark of 80% for each Functional Requirement Section (sheet).

4.2 Non-Functional Requirements (Compliance Requirements) – 7.50%

The Non-Functional Requirements (Compliance Requirements) of the Buyer are in questions 4.2 below.

For each of the Non-Functional Requirements (Compliance Requirements) there is a maximum word count of 500 (unless indicated otherwise in the question). (Any information provided in excess of the 500-word count will be disregarded. The 500-word count does not include text in diagrams or project plans).

Please see the Further Competition Instructions to Bidders paragraph 22.16.3 for the Non-Functional requirements (Compliance Requirements) detailed evaluation information including the marking scheme used for all of the questions in this section.

4.2 a)	Flexible Configuration	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
Your response should detail what elements of the solution allow configuration and those which do not. Please also describe where different specific 'multi tenancy' rules configuration is allowed. (e.g. audit selection per 3rd Party supplier, Individually branded Correspondence via SMS/Letter) Note: Configuration is considered to be control of the solution through the use of the native tools provided, without the development of bespoke customisation/components or code. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, detail how your solution will support administrative configuration to allow flexibility in the solution including describing how this flexibility is available at multi tenancy 'LOT' level,		
We confirm that our solution fully meets the requirement for Administrative Configuration, and that as this requirement is already available, it will be included within the Viable Product Release and by the Operational Service Commencement Date. We will integrate our present, robust capabilities with the Buyer's ServiceNow CMDB to enable the Buyer to manage multi-tenancy changes at the LOT level using only CMDB parameter changes (no further coding needed; see following). Our proposed solution is a significantly improved version of the current Atos platform enhanced with a new digital platform: both will have enhanced configuration management control in two key areas: 1. Within the Atos Web Gateway for Role-Base Access Control (RBAC) security control of platform users. Here, what is available to user groups, (for example, internal IAS users versus our Health professionals providing assessments for the Lots we are currently assigned) is controlled 2. Within the SAMS gateway for the Siebel Customer Relationship Management (CRM) sub-platform. Again, user group access to data sets (as an example, the CRM functionality/customer data provided to internal IAS users versus our Health professionals) is determined here. Given the Buyer's investments in ServiceNow and based on ServiceNow CMDB integrations done recently for two other clients, we will: • Effect control of what claimant data in each Lot can be seen by each third-party assessment provider all claimant data elements such as medical records, GP referrals and part/in-progress assessment will be included, along with other relevant third-party items, such as branded letters/SMS) using the Buyer's ServiceNow		

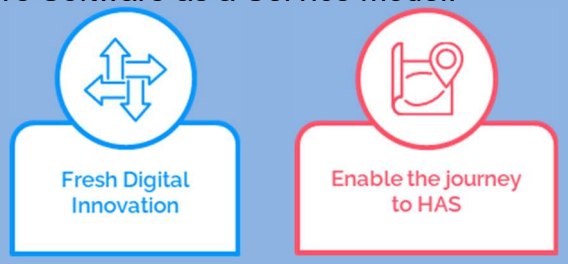
- As patients move about between Lot areas, exception handling will need to be agreed, but these outcomes will be configurable
- As an additional, improvement opportunity, before the Operational Service Commencement Date we will link our present configuration control functions (see above) to this functionality where there is sufficient joint value.

In line with Atos' general drive to digitise our service operations, the current delivery team has begun to convert our existing platform into a digital one, to provide:

1. New functionality that allows us to make the HPs more efficient, thus providing shared saving to the Buyer and the FAS providers
2. More efficient platform operations
3. Conversion of some functional components into micro services-based applications, which in turn can be re-used and integrated within the Buyer's planned HAS platform.

As soon as the contract is awarded, it is our intention to invest further in the digitalisation of the platform and ensure all required functionality is available no later than the Viable Product milestone.

Further, our Full Stack Engineering design and delivery techniques used here include consistent use of Continuous Integration/Continuous Delivery (CI/CD) pipeline techniques to facilitate configuration management and automated testing, where value is achieved, this approach will be integrated with the Buyer's ServiceNow, to optimise the configuration flexibility, moving both parties closer to an effective Software as a Service model.



475 words

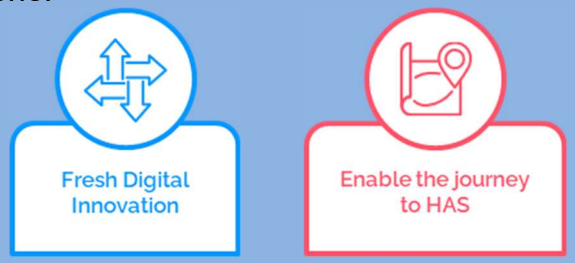
4.2b)	Application and Data Segregation	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
Your response should detail how your solution supports logical data separation at a Lot or Provider level. Users of the systems will, potentially, be split across numerous suppliers who will be allocated to Lots based of geographical regions. Therefore, a logical segregation of data and functions is required that will ensure access based upon business need. This logical separation based on Lot structures should be configurable to allow flexibility of the solution to allow changes in the allocation of cases across suppliers. The solution must enforce access via a robust RBAC (Role Based Access Control Q4.2m below) model that underpins the multi tenancy requirement. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, detail how your solution will be able to support 'Multi tenancy' with Users of the system only allowed access to data within their allocated Lot enforcing access via a robust RBAC model,		
We confirm that our solution fully meets the requirement for support of 'Multi tenancy' with Users of the system only allowed access to data within their allocated Lot enforcing access via a robust RBAC model. As this requirement is already available, it will be included for Viable Product Release and Operational Service Commencement Date. In short, we will be leveraging our present capabilities augmented by new multi-tenant functionality as described below; As outlined previously, we have an established Roles-Based Access Control (RBAC) method using Atos Web Gateway as part of the current platform. This method facilitates separation of internal IAS users and our health professionals for our geographic Lots to certain applications and (thus) logical data structures. For sub-platform elements based on either platform, Two-factor Authentication (2FA) is built-in. Our proposed solution is based on the current Atos Identity System solution as currently used within our DWP PIP support activities enhanced with a new digital platform. Both the current and the new digital platform already provide logical data structure separation for different users at an application and/or server level for claimant data in different geographic Lots. Based on our existing RBAC model, both are being extended to provide parameter-driven multi-tenancy support via the Buyer's ServiceNow. For the former platform, this base capability is provided by the Atos IRIS cloud platform product set and Oracle-base data structures. For the latter this is provided using AWS' industry leading capabilities in this area. Essentially this is done on both platforms by Relational Database structures keyed to the user role. If needed for resiliency/redundancy, physical separation can be provided on the digital platform by using both of AWS' physical zones in the UK.		

Our solution will provide RBAC-based logical data separation for each FAS provider, with the option of providing further separation for the new set of the Buyer's users (for example, based on those with clearance to see Personal Protected Information versus those who are not). Within these Lots, the user's defined role will determine the data they have access to based on business need (e.g., a Lot X Health Professional will have access to all data sets needed for PIP assessments within Lox X).

In line with Atos' general drive to digitalise our systems and service operations, the current delivery team has already begun to convert our existing platform into a digital one, to provide:

1. New functionality that allows us to make the health professionals supporting the Lots more efficient, thus providing shared saving for both the Buyer and FAS providers
2. More efficient platform operations/lower costs
3. Conversion of some functional components into micro services-based applications, which in turn can be re-used and/or integrated within the DWP's planned HAS platform.

From contract award, we will invest further in the digitalisation of the platform and ensure all required functionality is available no later than the Viable Product milestone.



478 words

4.2c)	Integrity Checks	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
Integrity checks must be applied at all stages of processing, where data is provided to or from other systems and integrated through the Potential Providers solution components. Where integrity checks fail, mechanisms must be provided to suspend processing of dataset, record the failure, and allow administrative intervention. In all cases transactional consistency must be maintained. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, detail how your solution will ensure transactional integrity and consistency at all stages of processing.		
We confirm that our solution fully meets the requirement for Data Integrity and that as this requirement is already available, it will be included for Viable Product Release and Operational Service Commencement Date. Our solution will refine the robust practices and methods we have in place in the current PIP operations enhanced with a supporting digital platform. • Our default practice concerning data integrity is to assume all data sources are untrusted and require validation • Data Integrity is most effectively managed using a multi-layer, “bottom up” approach (transmission level, data type/structure, specific data value(s)). The solution has three main data ingestion sources, with proven integrity checking at appropriate levels: 1. Ingestion of assessment support data, concerning which validation is the responsibility of the SAMS access control application gateway to the Oracle databases. The validity of patient data is in turn dependent on the quality of the input sources, ranging from OCR-readable text document (which we provide validity checks of key elements), to pictures of hand-written notes 2. Health Professionals supporting claim assessments via application input validation. Again, key elements needed for indexing and cross-referencing their inputs are validated, while some, more minor elements (e.g., comments) are not 3. Technical resources providing platform support functions. The user inputs from these resources are generally not edited, but their actions are logged for auditing as appropriate. The first two sources have a reasonable degree of data input validation support. In addition, multi-level integrity checking in the form of data path (e.g., XML schema validation) and platform/network (e.g., checksum on data packets) techniques are consistently applied. This validation level will increase given planned enhancements (described below).		

In line with Atos' general drive to digitise our service operations, the current delivery team has begun to enhance our existing platform with a new digital platform, to provide:

- New functionality that allows us to make the health professionals supporting the Lots more efficient, thus providing shared saving to the Buyer and the FAS providers
- More efficient platform operations
- Conversion of some functional components into micro services-based applications, which in can be re-used or integrated within the Buyer's planned HAS platform.

From contract award, we will invest further in the digitalisation of the platform and ensure all required functionality is available no later than the Viable Product milestone. With respect to this particular functionality, we will use machine learning techniques to pre-validate and index Claimant record documents for relevance to a health professional assessment, saving them up to 2 hours per case assessed based on user trials with other clients to date. The validation component of this effort can easily be modified to add further data integrity and protection checks, reducing the need for validation of entries by the health professionals themselves.

The Buyer can be assured that one of the key themes of our solution is to bring fresh digital innovation to our service and this will include enhancing the data validation.

484 words

4.2d)	Audit Events	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
The solution components must generate time-stamped audit events for every action that is taken, whether through administrative or user interfaces. Events created through any inbound interface also need to be audited. Audit events must be output/stored in a standard format with an agreed standard set of attributes. Note: Audit events include both successful and failed attempts to perform an action or access data. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, detail your audit event provisions for Healthcare Provider users, Buyer users (those interacting with the application interface) and Privileged system users (those accessing the underlying applications and Infrastructure components),		
We confirm that our solution fully meets the Non-Functional Requirement for Audit Events and that as this requirement is already available, it will be included for Viable Product Release and Operational Service Commencement Date. In short with respect to this functionality, we will be refining further the time-tested practices and methods we already have in place (as described below). As with our platform for the current DWP PIP support requirements and as applied for three other clients (e.g. ResRe), the proposed Microsoft Access Domain (AD) control solution provides authentication, authorization and audit services, enabling Single Sign On (SSO) for users into the system and services which make up the platform. The AD solution is supported by the Oracle Access Manager application, enabling SSO between all applications and data stores followed by determination of what data sets are made available to each user by Lot. Once that is determined, all user interactions regardless of role are time-stamped and logged by Access Manager to a separate log store within Oracle. The formats stored and the associated standard set of attributes have already been agreed with the Buyer. These logs are audited on a regular basis using semi-automated routines derived from those provided by the vendor, testing for Type I (direct, e.g. unauthorised person trying to gather PPI) and Type II (indirect, e.g. person repeatedly tries unauthorised actions for role) risks and providing these for further analysis and action. These logs and risk sources are also made available to the Buyer for their own analysis. In line with Atos' general drive to digitalise our systems and service operations, the current delivery team has already begun to convert our existing platform into a digital one, to provide: 1. New functionality that allows us to make the health professionals supporting the Lots currently assigned to us more efficient, thus providing shared saving to the Buyer and ourselves		

2. More efficient platform operations/lower costs
3. Conversion of some functional components into micro services-based applications, which in turn can be re-used and/or integrated within the Buyer's planned HAS platform.

From contract award, it is our intention to invest further in the digitalisation of the platform and ensure all required functionality is available no later than the Viable Product milestone. As part of this effort with respect to this functionality, by the Operational Service Commencement date we will implement industry-leading user level access control, data access, and auditing functionality provided as standard functionality from AWS once the digital platform enters the next stage of its introduction.

418 words

4.2e)	Identification of Audit Events	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
The solution components must generate time-stamped audit events for every action that is taken, whether through administrative or user interfaces. Events created through any inbound interface also need to be audited. Audit events must be output/stored in a standard format with an agreed standard set of attributes. Note: Audit events include both successful and failed attempts to perform an action or access data. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is not required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution will include an attribute to allow identification of all audit events of the user/service performing each action to meet our requirements,		
We confirm that our solution fully meets the Non-Functional Requirement for identification of audit events and that as this requirement is already available, it will be included for Viable Product Release and Operational Service Commencement Date. In summary here, we will be refining further the robust practices and methods we already have in place and as worked out with the Buyer. As currently performed on behalf of the Buyer and other clients (e.g. [redacted] [Redacted FOIA S43 Commercial Interest]), all user actions with the proposed platform are time-stamped, logged and audited regardless of role. These include both successful and failed attempts to perform an action or access data. Similarly, Active Directory (AD) is used to provide logging of PIP assessment data input sources to PRS, which are then put to the same Oracle log data store using timestamps and event attributes that have been agreed with the Buyer. These logs are audited on a regular basis using semi-automated routines derived from those provided by the vendor, testing for Type I (direct, e.g. data input isn't relevant to an assessment) and Type II (indirect, e.g. input source repeatedly tries unauthorised actions for role) risks and providing these for further analysis and action. Like for users, these logs and risk sources are also made available to the Buyer for their own analysis. In line with Atos' general drive to digitalise our systems and service operations, the current delivery team has begun to convert our existing platform into a digital one, to provide: 1. New functionality that allows us to make the health professionals supporting the Lots currently assigned to us more efficient, thus providing shared saving to the Buyer and ourselves 2. More efficient platform operations 3. Conversion of some functional components into micro services-based applications, which in turn can be re-used and/or integrated within the Buyer's planned HAS platform.		

From contract award, we will invest further in the digitalisation of the platform and ensure all required functionality is available no later than the Viable Product milestone. With respect to this functionality and in line with similar efforts for other customers, we plan to use machine learning techniques to pre-validate and index patient record documents for relevance to a PIP Health Professional assessment, saving them a up to 2 hours per case assessed based on user trials for other customers to date (e.g. HMRC) . The validation component of this effort will be modified to add the current auditing efforts in an automated way.

408 words

4.2f)	Audit Event MI	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
Data transactions must record sufficient tracking information against them such that all data, individually and in summary, can be accounted for throughout its journey through the solution. This must include a timestamp when, for example, process(s) started and finished or when an update was written. In the event of error, reasons for failure must be available in sufficient detail to aid their resolution. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is not required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution will meet our Audit Event MI requirements.		
We confirm that our solution fully meets the Non-Functional Requirement for Audit Event MI, and that as this requirement is already met within the current operational service, it will be included for Viable Product Release and Operational Service Commencement Date. Our solution is based on the AIS platform that has been supporting the Buyer's (and Atos's) auditing requirements for logging user and input transactions for several years. Atos is confident all of the Buyer's requirements are met with respect to time stamping, event attributes (e.g. start, stop, when written, etc.) and system failure reason(s). PRS captures a full audit history covering when users have created or updated a data record, or even just accessed that record on a page. This comprehensive audit trail enables tracking of, for example, all activity undertaken in connection with a given claimant. It will also enable reporting and analysis of all activity undertaken by a given user, detailing each function executed on each screen in respect of which NINo (or customer reference number), together with a timestamp. This also covers searches and read access as well as update transactions. The SAMS application offers equivalent functionality using standard 'out of the box' Siebel features. All of this audit data is stored in the Oracle databases and will be available from the Atos IT support team by authorised request. Start and end times for processes are logged for user interactions such as saving or submitting and assessment report, calls to the various rules engines and workflow progression events, as well as batch jobs such as IF7/IF8 processing, letters jobs and end-user data uploads. Atos confirms that error events, including reasons for failure, are captured in sufficient detail to aid investigation and resolution. Application logs capture all events such that any errors are recorded together with diagnostic information explaining exactly where in the application it occurred (i.e. which line in the code caused the issue). Issues are categorised into errors, warnings, with an option to flag debug messages. The Atos IT support team will investigate PRS and SAMS errors		

and warnings through routine daily checks and monitoring. Where appropriate, debug mode can be switch on 'on the fly' (i.e. without interruption to end users) to provide capture a level of diagnostic information.
The Digital Platform refers to Atos's public cloud hosted environment for secure enterprise consumption of AWS services. This platform has the potential to support the Buyer's development of the future HAS platform by showcasing our vision and capability to deliver fully cloud first, native applications. Code from this Digital Platform can be used by the HAS team and ported into the HAS platform as required. New PIP IT functional requirements will be assessed and, if appropriate, developed on this platform in line with Atos's drive to digitise customer systems and service operations. Where new functionality is not appropriate for the Digital Platform, Atos will fully meet the Buyer's requirements through enhancement to the existing PRS, SAMS and MIS applications.

493 words

4.2g)	Non-Production and Training Environments	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must include provision for testing system changes through deployment of distinct, and isolated from Production, Non-Production environment(s). The Non-Production environments must support regular functional, regression, performance, accessibility, operational acceptance, user acceptance, service management and transition and prod-fix testing, using automated testing tools to inform quality management processes prior to releasing configuration changes into Production. All user testing environments must be capable of being accessed from the same End User Devices as production services The solution should also support the capability for a discreet training environment to support training of the users of the system, this must be segregated from Production and not use live data, it must be capable of being accessed from the same End User Devices as production services. Please include details of any licensing requirements which would apply to Non-Production or training use. Note: Non-Production refers to all environments outside Production. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution will meet our Non-Production and Training environments requirements.		
Our solution fully meets the requirements for Non-Production and Training Environments. These essential capabilities are already available within our existing services, which provide the foundation capabilities within our proposed solution, to be refined and enhanced to address the Buyer's additional requirements. This will minimise the development required, enabling us to confirm that these capabilities will be included for Viable Product Release and the Operational Service Commencement Date. Building on our current platform, we will provide separate environments for support of non-production and training activities. These environments include those we use for development, and those we make available for training and all aspects of to-production testing. All are physically and/or logically separate from the production environments. These platforms will be available using the same access methods to those used in our production environment(s), and can be set up to use live, static, dummy and/or obfuscated data, depending on use case. These non-production and training platforms are grouped for supporting two user sets and their related needs, as follows: 1. Atos platform support users. This user set performs unit, functional, regression, performance, accessibility and production fix testing on their platforms		

2. All other users: This user set performs accessibility testing, along with operational acceptance, user acceptance and service management activities. Testing support in line with what is used for the previous user group and for production is supported here as well.

In line with Atos' general drive to digitalise our systems and service operations, the current delivery team has begun to convert our existing platform into a digital one, to provide:

1. New functionality that allows us to make the health professionals supporting the Lots currently assigned to us more efficient, thus providing shared saving to the DWP and ourselves
2. More efficient platform operations/lower costs
3. Conversion of some functional components into micro services-based applications, which in turn can be re-used and/or integrated within the Buyer's planned HAS platform.

Our solution incorporates our Full Stack Engineering design and delivery techniques, including consistent use of Continuous Integration/Continuous Delivery (CI/CD) pipeline techniques, to facilitate state-of-the art design, delivery and fully automated testing, allowing matching of code base, data and non-production functionality done to an individual function set as needed. Using this approach and the flexibility of AWS infrastructure used within the digital platform, Atos can provide non-production environments for individual and/or functional needs as desired, along with capturing them for re-use at any time (i.e. it is possible to make the testing environment consistent for each trainee, and have it recreated or adapted for others very quickly).

424 words

4.2h)	Backup Processes	Weighting 0.20% Aesthetic & Functional Characteristics
Guidance:		
The solution must support automated backup and restore procedures for all application configuration, user data and audit data. Note: Backup processes could be initiated with ongoing user access, API access or whilst scheduled batch and/or real-time processes may be executing. Transactional consistency must be maintained across the entire solution for each point-in-time backup data set. Backup data has the same level of security control as the original data. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe your solutions Backup processes to meet our requirement.		
Our solution fully meets the requirement for Backup Processes. As these essential capabilities are already available within our existing services, these capabilities will be included for Viable Product Release and the Operational Service Commencement Date. Given this context, our proposed solution includes a set of established and trusted backup procedures for each critical element (applications, system and user databases, CRM, etc.), crafted in a manner whereby all end-to-end platform transactions are retrievable in a consistent way and at agreed points in time. These procedures will continue, whilst being refined or enhanced where necessary. The backup regime will include: • Back-up of the application set via a batch job weekly and/or at run-time when material changes are made (for example, application releases, supporting software hotfixes, etc.) • Back-up of Oracle databases via a batch job to suitable storage media each weekday, based on Business Day availability of the platform (with run-time updates synched to application changes also) • Back-up of the Siebel CRM configuration files via a batch job on a weekly basis, with run-time updates in synch with the above data sets. Run-time changes are initiated using both existing user and API methods. Using the same tools and methods, all back-up methods are constructed in a way that ensures all backed up data has the same security level as applied to the original data sets. Where appropriate (e.g. data bases) these are done to provide transactional consistency; in other words, a restoration path in the event of an infrastructure or communications failure, or to get back to a “safe point in time” if an issue is found in production with a material change (e.g. application release, supporting software hotfixes, etc.).		

We have already begun to convert our existing platform here into a digital one, to provide:

1. New functionality that allows us to make the health professionals supporting the Lots currently assigned to us more efficient, thus providing shared saving to the Buyer and ourselves
2. Through the latest design/delivery techniques, more efficient platform operations/lower costs
3. Conversion of some functional components into micro services-based applications be which in turn can re-used within the Buyer's planned HAS platform.

We also incorporate redundancy, reducing any reliance on a reversion to back-ups:

The proposed relational and non-relational databases to be used have built in resilience across availability zones using standard AWS functionality. Redundant configuration that switches to the backup databases automatically when an issue is identified, while providing another path away from third-party software dependence.

The proposed CI/CD pipeline methodology and toolkits used both keep each software change made in a resilient, redundant configuration for roll-back in case of an issue, as well as providing an automated test suite that reduces the effect of problematic changes and output defects by a factor of 10.

Our solution approach will capture and build on existing work and projects to enhance resilience and improve 'back-up' capabilities, including efforts to provide further CRM functionality using micro-services.

487 words

4.2i)	Upgrade Process	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
The Potential Provider must provide a documented upgrade process for any future releases. This must cover all hotfix, minor and major releases where applicable. The documentation must include a reversion process should the upgrade require reverting at any point up until the upgrade becomes operational. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, document the future upgrade roadmap of your solution		
We confirm that our solution fully meets the requirement for Upgrade Process. This will be included for Viable Product Release and the Operational Service Commencement Date. Upgrade Process Fully documented processes cover all aspects of the upgrade process. This covers the following process stages: • Development and unit test • System testing • Integration testing • Performance testing (where appropriate) • User acceptance testing • Live proving • Deployment into production • Confidence testing. Live proving takes place in a staging environment which is an exact replica of the production environment, providing confidence that the system upgrades function exactly as expected. Once all tests have been passed satisfactorily, within this staging environment, the changes are then deployed into production. Immediately following deployment, business users then conduct controlled and pre-planned confidence testing to provide final assurance that the deployment is functioning correctly. In the event that any issues are identified that warrant rollback, the reversion process is then followed. Reversion Process Where the business release manager makes the decision to roll back following issues identified during confidence testing, the reversion process is executed. This involves the restoration of backups of the live applications and the execution of roll-back scripts to undo any data changes made either as part of the deployment or during confidence testing in production. In		

exceptional circumstances where such rollback of data updates is not successful, then a full database backup will be restored. This provides the assurance that data will not be lost in the event of a failed upgrade, and that service continuity is protected.

Upgrade Roadmap

There are some key technical upgrades planned for June 2022, most notably an Oracle upgrade for PRS, an upgrade to the SAMS application to support this new version of Oracle, and an upgrade to PRS for compatibility with Chrome (required because IE11 reaches end of life).

Our solution also incorporates a series of functional releases to deliver the Buyer's functional requirements through the planned work packages listed below:

(1)	Package	(2)	Content/Theme
(3)	WP0	(4)	AD users and privileges into Siebel component
(5)	WP1	(6)	Alternative format comms & SMS to claimant on referral receipt
(7)	WP2	(8)	Assessment tool improvements, including replacing PDF input forms with Java UI
(9)	WP3	(10)	GPFR payments and ad hoc system-generated letters
(11)	WP4	(12)	IF6 interface to fully automate all aspects of the closure process
(13)	WP5	(14)	Multi-tenanting
(15)	WP6	(16)	Allocation of workflow-related tasks (supplements existing self-allocation with push/reallocate)
(17)	WP7	(18)	Welsh notifications, suppression of military titles & additional SMS reminders
(19)	WP8	(20)	DWP/DfC access to PIP IT (case management and MI systems)
(21)	WP9	(22)	Auto-approval of low-value expense claims
(23)	WP10	(24)	Ad hoc task creation with 'get next' self-allocation
(25)	WP11	(26)	IDV validation rules and sending draft assessment reports to DWP Document Storage Solution
(27)	WP12	(28)	Ad hoc task allocation (supplements self-allocation with push/ reallocate)
(29)	WP13	(30)	User questions on FE covering letters, short notice appointment letter variant & expense forms

Multiple work packages may be deployed in a single release. Our proposal is to deliver these changes to IAS users in the period leading up to Viable Product Release, to minimise training and reduce overall programme risk.

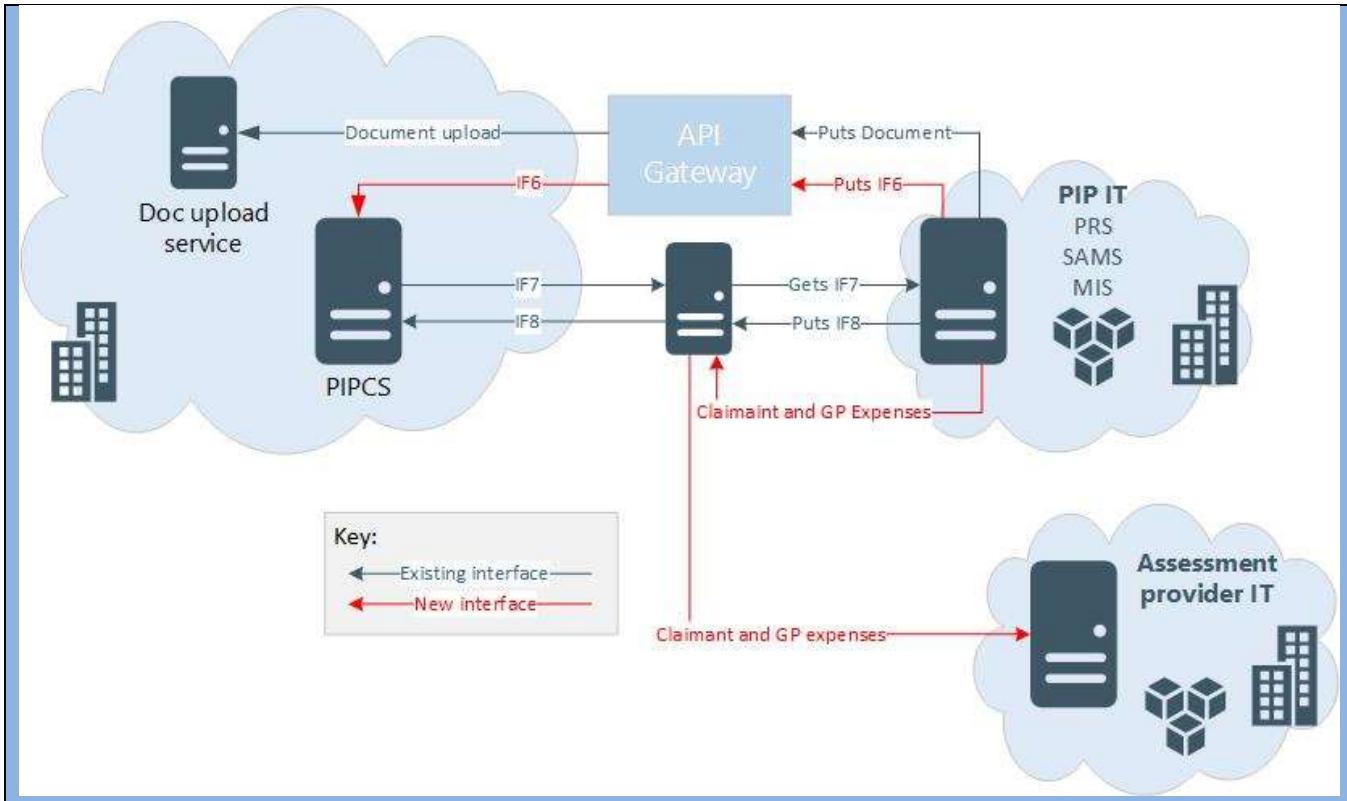
499 words

4.2j)	Backward Compatibility	Weighting 0.10% Aesthetic & Functional Characteristics
Guidance:		
The solution must provide backward compatibility across all APIs for all hotfix and minor upgrade releases. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution will ensure backward compatibility.		
We confirm that our solution fully meets the requirement for Backward Compatibility across all APIs for all hotfix and minor upgrade releases. As this is already catered for within the system, it will be included for Viable Product Release and the Operational Service Commencement Date. Wherever possible, this backwards compatibility is also routinely provided for major releases, not just hotfixes and minor releases. Development in areas of the solution that will integrate with other systems (e.g. IF6/7/8, document uploads to DRS and payment instructions for Assessment Provider systems for GPFR invoices and claimant expenses) will explicitly factor in the necessary provisions for backwards compatibility. Development and test cycles will include older versions to ensure that they are compatible and can continue to be consumed successfully. 'In flight' cases (i.e. referrals already in progress) will always be tested to flush out instances where, for example, it may not be possible to populate a new mandatory field. Specific provision will be made in the solution design for all such compatibility issues. The Atos team that will design, build and operate the solution has considerable experience of successfully identifying and managing backwards compatibility issues. For example, our solution's Offline Assessment Tool (OAT) uploads data through a PRS API. This always designed for, and tested against, previous versions. The benefit of this is the assurance of knowing that offline reports produced on older versions of OAT will still be imported successfully to the online system and will navigate downstream processing as required. The interface API processes the incoming data taking account of the specific version and responding accordingly. Backward compatibility will also be available within our Digital Platform that will be used for new functionality. The Digital Platform refers to Atos's public cloud hosted environment for secure enterprise consumption of AWS services. This platform has the potential to support the Buyer's development of the future HAS platform by showcasing our vision and capability to deliver fully cloud first, native applications. Code from this Digital Platform can be used by the HAS team and ported into the HAS platform as required. New PIP IT functional requirements will be assessed and, if appropriate, developed on this platform		

in line with Atos's drive to digitise customer systems and service operations. Where new functionality is not appropriate for the Digital Platform, Atos will fully meet the Buyer's requirements through enhancement to the existing PRS, SAMS and MIS applications.

400 words

4.2k)	Interfaces with Other Systems	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must integrate with multiple Buyer and Healthcare Provider systems, and include design and development of integration components. The solution must be capable of providing Management Information data to the Buyer. Healthcare Provider system integration must be using standard methods and standard format of output, this will include but not limited to Expense Payment Fulfilment and GP Further Evidence payments. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, your response should include all High Level interface documentation required to meet our requirement, including any Buyer obligations for any interfaces.		
We confirm that our solution fully meets the requirement for interfaces with other systems, and that this requirement will be included within the Viable Product Release and for the Operational Service Commencement Date. This extends to the provision of all appropriate high level interface documentation. Our proposed solution, which builds upon the systems in operation today, has been designed with flexibility in mind to be able to easily integrate with external systems. The diagram below shows existing and proposed new interfaces:		



The current solution interfaces with the Buyer's API Gateway to allow for the communication and the sharing of data between the Buyer's systems and Atos's systems. This includes:

- IF7 transactions from PIPCS to PIP IT (for new referrals and CoCs from the Buyer)
- IF8 transactions from PIP IT to PIPCS (for CoCs from APs)
- DRS upload from PIP IT to DRS (for PDF files including completed assessment reports).

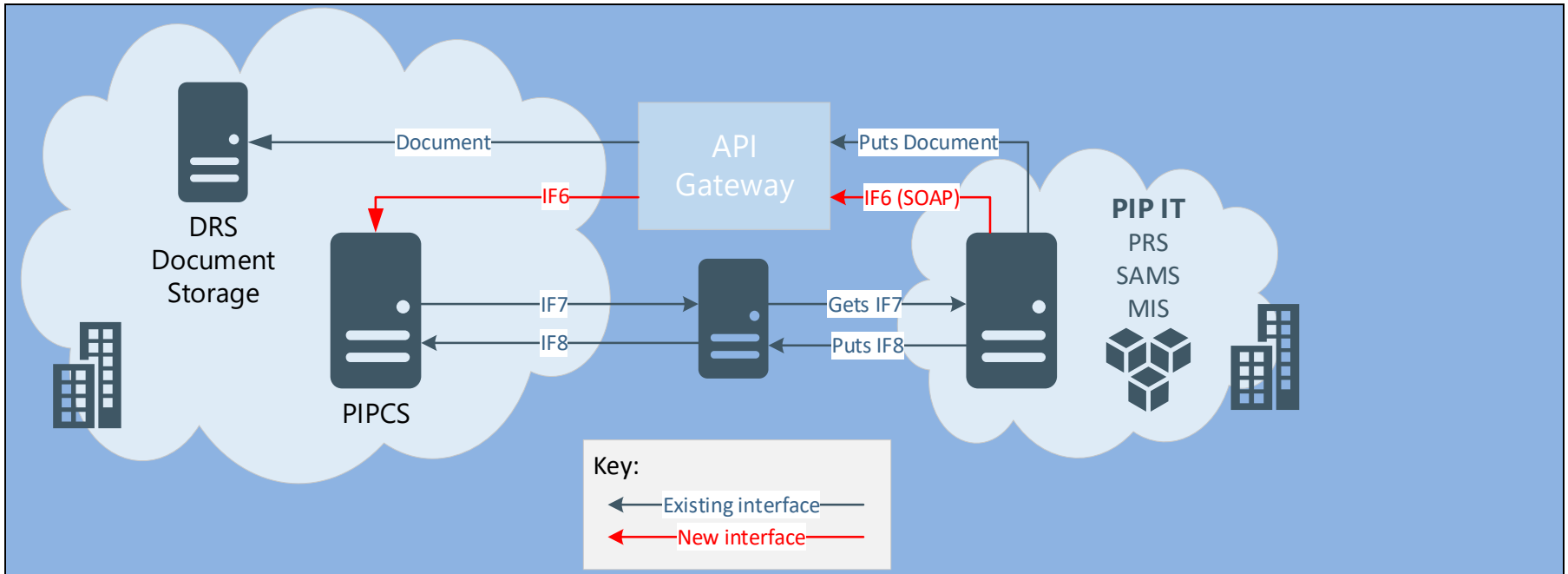
Our solution's established IF7 processing ingests XMLs from PIPCS to PRS both overnight and at regular intervals throughout the day. IF8 processing creates XMLs conformant to the Buyer's specification and sends these to PIPCS in regular batches. The more recently implemented DRS upload interface uses a RESTful API to pass PDF documents to DRS throughout the day. These interfaces are currently live and well-established, offering a reliable, low-maintenance, and successful method of interfacing with the Buyer's systems. Atos will expect the above interfaces to continue to be made available to our solution by the Buyer.

Our solution will support use of the Buyer's existing IF6 SOAP interface to PIPCS via the same external-facing Buyer API gateway as used by the existing document upload service. Our proposal includes the necessary design and development of these integration components.
We will also be providing new interfacing from Atos systems to Healthcare Provider systems. Specifically, claimant expense payment instructions will be generated from SAMS and GPFR payment instructions will be generated from PRS. Each will create lot-specific files that will be placed in a destination to be agreed with the Buyer, from where the data can be consumed by appropriate Healthcare Provider systems. The files will be placed there in nightly batches in XML format and will conform to specifications that Atos will agree with the Buyer.
Our solution will provide management information (MI) to the Buyer and Healthcare Providers through direct access to the Cognos portal through the Zscaler solution, and through that, access to the standard MI reports as covered in the Buyer's functional requirements, plus the ability for users to generated ad hoc reports on demand. This direct access offers maximum flexibility and ensures that all users of this data are able to benefit from having the most up-to-date information at any time.

The Buyer can be assured that one of the key themes of our solution is operational stability and security.

470 words

4.2l)	Integration with Existing Systems	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must integrate with multiple existing Buyer systems, and include design and development of integration components. The solution must be capable of processing the existing Buyer integration XML files from PIP CS (IF7 and IF8) and RESTful API's (Document Upload Service) to minimise change to the current Buyer systems that support the service. The new PIP IT solution should also support use of an existing SOAP PIP CS interface (IF6) available to automatically update the PIP CS system with assessment outcomes. This interface is not currently used by external systems to the Buyer but will be made available for use in the future via the external facing Buyer API gateway. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, your response should include all High Level interface documentation required to meet our requirement, including any Buyer obligations for any interfaces.		
We confirm that our solution fully meets the Non-Functional Requirement for interfacing with existing Buyer systems, specifically: • IF6 transactions from PIP IT to PIPCS (for referral outcomes) • IF7 transactions from PIPCS to PIP IT (for new referrals and CoCs from DWP) • IF8 transactions from PIP IT to PIPCS (for CoCs from APs) • DRS upload from PIP IT to DRS (for PDF files including completed assessment reports). All of these will be available for Viable Product Release and for the Operational Service Commencement Date. Other than IF6, each of the above is currently live, well-established, and supporting the business operation for Lots 1 and 3. Our solution proposes no changes to their existing design or implementation. The diagram below shows all four interfaces in context, indicating the direction of data flow:		



Our solution's established IF7 processing consumes large files received from PIPCS overnight and smaller files received throughout the day. Each of these is consumed whilst our system continues to support AP end-user activity. Our solution creates XML files for nightly transmission to PIPCS containing CoC notifications created by AP users. The more recently implemented DRS upload interface uses a RESTful API to pass completed assessment reports and other documents in PDF format, along with all pertinent metadata as agreed collaboratively with DWP Digital colleagues, to DRS throughout the day. This has proven to be hugely successful, eliminating the latency of the old 'print, van and scan' approach whilst also contributing significantly to decarbonisation.

Our solution will support use of the Buyer's existing IF6 SOAP interface to PIPCS via the same external-facing Buyer API gateway as used by the existing document upload service. Our proposal includes the necessary design and development of these integration components.

It is both our intention and our expectation that this will be achieved with no changes to the Buyer's existing IF6 Data Definition. Atos has already raised detailed questions on IF6 content during this procurement (CQ97) and shares the Buyer's pragmatic approach that mandatory fields be set to dummy values where source data is legitimately not held (e.g. HP details in certain scenarios).

Atos will need the Buyer to engage in the validation of high-level and detailed design artefacts, and to make provision for end-to-end integration testing of the new interface. Given the success of collaborative working between the Buyer and Atos

in the implementation and continued live running of IF7, IF8 and the recently-introduced Document Upload interface, Atos is very confident of a successful delivery. Having had sight of the IF6 interface definition during this procurement, Atos is further assured and has no particular concerns with the data requirements it contains.
Where appropriate, new functionality will be developed on the Digital Platform (Atos's public cloud-hosted environment for secure enterprise consumption of AWS services) in line with Atos's drive to digitise customer systems and service operations. Where new functionality is not appropriate for the Digital Platform, Atos will fully meet the Buyer's requirements through enhancement to the existing PRS, SAMS and MIS applications.

497 words

4.2m)	Role Based Access Control	Weighting 0.30% Aesthetic & Functional Characteristics

Guidance:

The solution must support Role Based Access Control (RBAC), whereby the Buyer's and Healthcare Provider user's capabilities within the solution are restricted to those defined specifically to their job role(s).
This requirement is required for Viable Product Release (See Attachment 6.1)
This requirement is required for Operational Service Commencement Date (See Attachment 6.1)

Question:

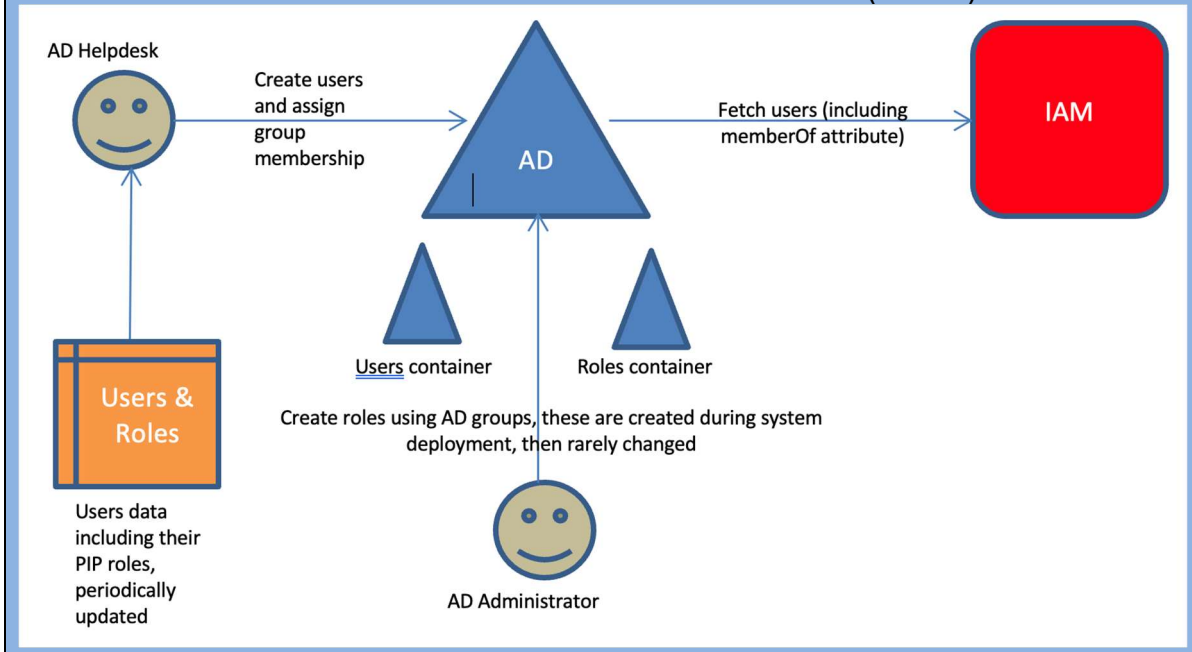
Incorporating the guidance above, describe how your solution authorises and controls user access to functionality and data on the basis of least privilege.

We confirm that our solution fully meets the requirement for Role-Based Access Control (RBAC), authorising and controlling user access to functionality and data on the basis of least privilege. This will be included within the Viable Product Release and for the Operational Service Commencement Date.
Security is a cornerstone feature of Atos' commitment to its clients and has been a critical consideration for the development of our solution. Since there is a wide range of actors and roles required to support the PIP assessment process, each with varying responsibilities and levels of access needed, RBAC has been deployed effectively within the solution, successfully ensuring that each user has only the minimum level of access required to successfully complete their given role. Some examples include:

- only 'HP' users can create or amend assessment reports
- only 'auditor' users can conduct clinical quality audits
- only 'lead auditor' users can respond to requests for expert help or to escalations
- only audit managers can abandon audits before completion
- only 'team manager' users can update HP diary/rota information
- only 'business support' users can process IF7 rejections
- only 'expenses administrator' users can input expense claims
- only 'resource manager' users can upload/amend appointment slots.

To meet the Buyer's functional requirements to support multiple APs (MISC_02 and MISC_03), we will enhance the RBAC restrictions within the applications to ensure that users will only have access to referrals that belong to the same contractual 'lot' as the user. For maximum flexibility, recognising the possibility that one AP could be contracted to deliver services across more than one lot, our solution will accommodate each user being associated with one or more Lots within Active

Directory (AD). New application logic will be built to allow users to access only referrals associated with any lot to which they themselves are associated.
Atos has successfully implemented exactly this kind of application logic to restrict access to referrals between DWP and DfC users within the MSRS system, which Atos continues to support under the ASIS contract for the Buyer.
To meet the Buyer's functional requirements to support read-only access for the Buyer and DfC users (MISC_04 and MISC_05), we will enhance the RBAC restrictions within the applications to create a new fully read-only user group.
As illustrated below, our Identity Access Management (IAM) solution provides authentication, authorisation and audit services, enabling Single Sign On (SSO) for users into the system and services. The IAM solution is based on Oracle Access Manager (OAM), enabling Single Sign On between all applications as well as providing a higher level of security by removing the need to continually send user ID's and password across the network. OAM uses an AD interface to check user credentials and determine and control the roles and access (RBAC) these users have been provisioned.

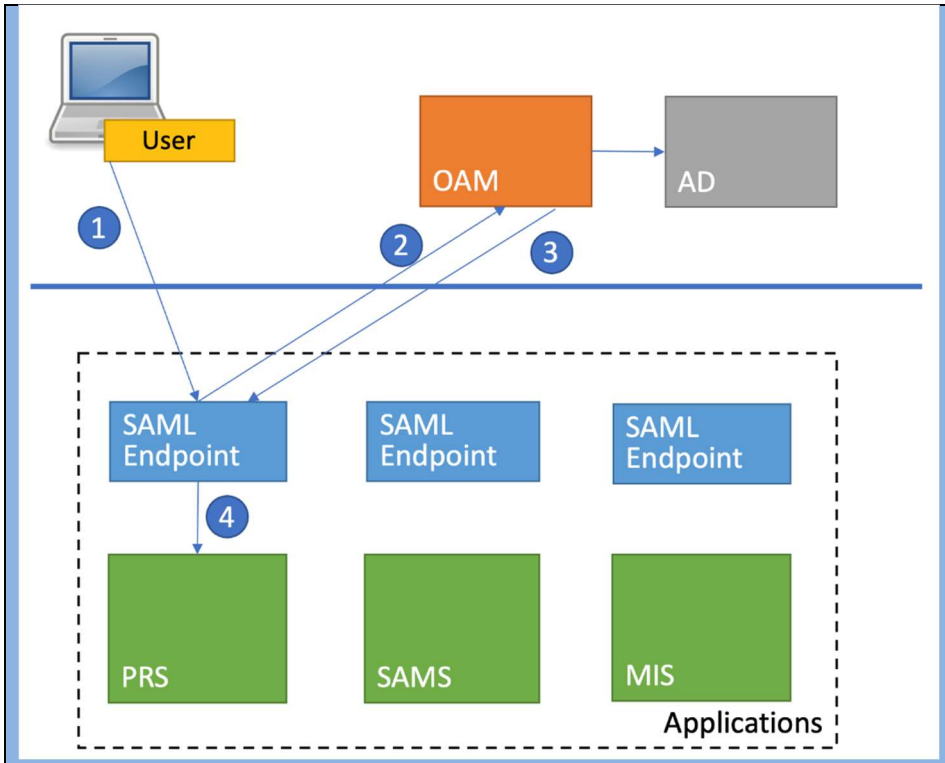


We will ensure that, where appropriate, source code for various systems is stored on a secure, private GitHub repository to provide source control and ensure that any changes made to source code can be easily managed and tracked.

Fresh Digital Innovation
Operational stability and security

498 words

4.2n)	Federated Identity Management	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must be SAML aware to enable authentication of user access. The solution will authenticate the users of the system via SAML token but fine grained access to roles and underlying data attributes must be provided as part of the solution for specific user's authorisation to functionality and/or data. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution meets our requirement to ensure authentication of users via SAML.		
We confirm that our solution fully meets the requirement for Federated Identity Management, and that this will be included within the Viable Product Release and by the Operational Service Commencement Date. In particular, our solution is able to authenticate users via SAML to ensure an easy and secure entry into various systems that are a part of the overall solution. Rather than share credentials, SAML enables the communication between identity providers and service providers using secure tokens (encrypted, digitally signed XML-certificates). This allows users to access multiple applications with trusted information and, by implementing single sign-on, to only log in once. SAML removes user error (i.e., weak or forgotten passwords), improves user experience by not requiring credentials for multiple applications, and does so securely. At present, our solution currently in operation for the PIP service is able to securely authenticate users using SAML or via Oracle Access Management (OAM). The SAML endpoints communicate with the Access Manager server using the secure Oracle Access Protocol (OAP).		



SAML endpoints will sit in front of the web services. If the user does not have a valid token to access the application, they will be redirected to OIF (Oracle Identity Federation), which will challenge the user via a web form for their AD credentials. After their credentials have been validated, they will be granted entry to the application via the SAML endpoint.
Policies are created and maintained by administrators through the Oracle Access Management console, which acts as the central Policy Administration Point (PAP). These policies are stored in the Policy Store on an Oracle database.
As an authenticated user tries to access different applications and resources, the runtime Access Manager Server acts as Policy Decision Point (PDP) evaluating whether the user is authorized to access a particular resource. It then conveys that information back to OIF which generates a SAML assertion for the endpoints. Every action gets logged for audit purposes.
Furthermore, for external federation, we will use OIF as a breakout point to generate SAML assertions for authentication to and from external entities.
We will also be using Role-Based Access Management (RBAC) to offer a further level of control and fine-grained access to users alongside SAML; this will be convenient for administrators to manage control and access for users of the applications.

Operational stability and security

The Buyer can be assured that one of the key themes of our solution is operational stability and security.

399 words

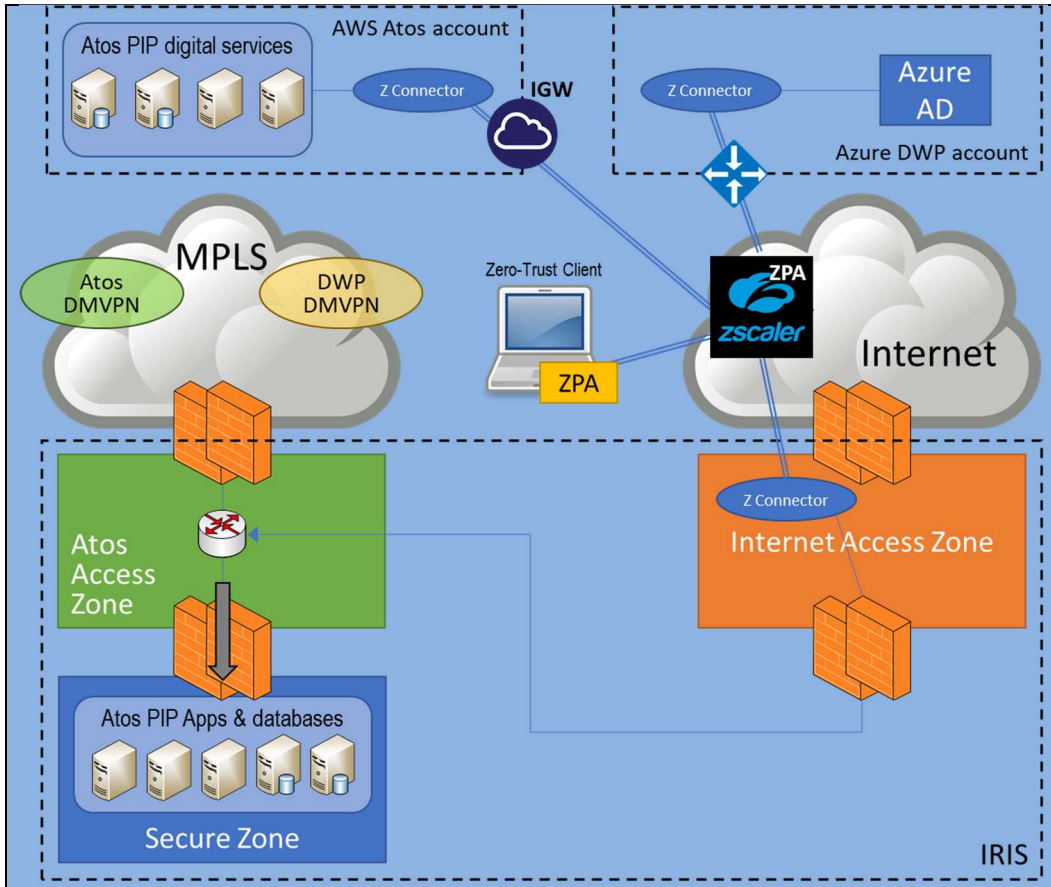
4.2o)	Buyer User Access	Weighting 0.20% Aesthetic & Functional Characteristics
Guidance:		
The solution must support access using the Buyer's standard browser (supported version(s) of Microsoft Edge), for all agent user functionality. Note: The Buyer end user device is based on a secure locked-down Microsoft Windows 10 operating system, using Edge Chromium browser (currently Version 85.0.564.44). This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution meets our requirement to ensure access is allowed from a standard Buyer End User Device.		
We confirm that our solution fully meets the requirement for Buyer User Access for all agent user functionality, and that this requirement will be included within the Viable Product Release and by the Operational Service Commencement Date. We know that the Buyer end user device is based on a secure locked-down Microsoft Windows 10 operating system, using Edge Chromium browser (currently Version 85.0.564.44). As such, we will be ensuring complete compatibility in our solution for your current hardware and software. In particular, the Zscaler solution used to access the platforms will be fully compatible with the Edge Chromium browser, giving all users of the system (with the approved hardware) simple and secure access to complete their roles. The Identity Access Management (IAM) solution which forms part of our solution provides authentication, authorization and audit services, enabling Single Sign On (SSO) for users into the system and services. Users will connect via a ZScaler VPN and Oracle Access Manager (OAM), which will use an Active Directory interface to check user credentials and determine and control the roles and access (RBAC) these users have been provisioned. This new system access for the Buyer's and DfC agents will provide them with read-only access to a range of information that will help those users respond quickly and effectively to claimant enquiries such as progress chasing. Users will be able to search on NINo or customer reference number to view referral details, a claimant's full appointment history and contact history, HP activity including FE gathering and initial review, and progress through clinical quality checking processes. This will greatly support the claimant experience and avoid generating unnecessary hand-offs to APs to provide that information. Any further development of new features required by the Buyer will also be thoroughly tested using the required device operating system and browser (i.e. Windows 10 and the Edge Chromium browser) to ensure compatibility. Furthermore, testing can be automated using CI/CD pipelines to specifically test using these platforms. In addition, we will ensure we avoid browser-specific code to maximise compatibility.		

New PIP IT functional requirements will be assessed and, if appropriate, developed on new, Digital platform (Atos's public cloud hosted environment for secure enterprise consumption of AWS services) in line with Atos's drive to digitalise customer systems and service operations. Where applicable, applications built for the Digital platform will be tested using the Buyer's required operating system and browser to ensure compatibility. This platform has the potential to support the Buyer's development of the future HAS platform by showcasing our vision and capability to deliver fully cloud first, native applications. Code from this Digital Platform can be used by the HAS team and ported into the HAS platform as required. Where new functionality is not appropriate for the Digital Platform, Atos will fully meet the Buyer's requirements through enhancement to the existing PRS, SAMS and MIS applications.

The Buyer can be assured that one of the key themes of our solution is operational stability and security.

494 words

4.2p)	Healthcare User Access	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must support user access by the Healthcare Provider users from the Buyer provided 'Cloud First' end user environment. Note: The Cloud First platform is built as a Windows 10 zero trust client and inherently bequeaths no trust to the local network provision. Instead it secures all communications (via Zscaler) using Azure AD. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution meets our requirement to ensure access is allowed from Buyer Cloud First Devices.		
We confirm that our solution fully meets the requirement for Healthcare Provider User Access, and it will be included within the Viable Product Release and by the Operational Service Commencement Date. Secure, yet simple, connectivity to the Buyer's platforms is a critical component of our solution. We know that the Healthcare Provider users will be issued with Buyer-approved Windows 10 devices, built on a Cloud First platform with a Zero Trust client that assumes no trust to the local network provision; hence, all connectivity from Healthcare Provider users to any Buyer platforms will be made securely via Zscaler using Azure Active Directory (AD). As such, we will be ensuring complete compatibility in our solution with all relevant applications for the hardware you will provide to Healthcare Provider users. We will work with you on implementing the Zscaler solution to ensure we meet your requirements. Zscaler Private Access (ZPA) secures remote working inbound access to internal company-owned technology resources, including applications hosted either in a data centre and/or a private cloud environment(s). Atos has a strong track record in implementing Zscaler solutions to our clients. For example, we successfully implemented a large-scale Zscaler solution for connectivity across user groups all over the world for the BBC. Access to Atos' IRIS data centre and/or private digital cloud platform, which will host our solution, can be facilitated by Z Connectors. IRIS is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads. Z Connectors enable secure communication between a Healthcare Provider user's device and the application. These Z Connectors, belonging to the Buyer's Zscaler tenancy, are deployed as virtual machines in resilient pairs within Atos environments. If required, traffic from the Z Connector to services and applications hosted within Atos environments may be further restricted on destination addressing and ports to allow for a more granular level of user access.		



The inherent security of the Zero Trust network will further ensure fast, secure access to cloud applications and will ensure that both the Healthcare Provider user devices and the Buyer's network remains secure and protected.
Furthermore, any further development of new features required by the Buyer will be thoroughly tested using the required Healthcare Provider user device operating system and browser to ensure compatibility. Additionally, testing can be automated using CI/CD pipelines to specifically test using these platforms.
New PIP IT functional requirements will be assessed and, if appropriate, developed on the new Digital platform (Atos's public cloud hosted environment for secure enterprise consumption of AWS services) in line with Atos' drive to digitise customer systems and service operations. Where applicable, applications built for the Digital platform will be tested using the Healthcare Provider users' required operating system and browser to ensure compatibility and will also be compatible with the Zscaler solution.

The Buyer can be assured that one of the key themes of our solution is operational stability and security.

489 words

4.2q)	Browser Compatibility – HTML5	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The agreed Buyer strategy for application development is that all client side presentation should be within a browser leveraging HTML5 for a richer User experience (including media if appropriate) and off-line capabilities. Client side development should focus on the core HTML capability with an aim of being browser and platform agnostic (including mobile devices); enabling the department to introduce new client devices in the future. Client-side scripting should be avoided as the Buyer strategy is for a device agnostic solution that is delivered via HTML5 and remains browser agnostic. Note: The Buyer only supports ActiveX and Browser Helper Objects (such as Silverlight) for legacy systems or by exception. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, detail how your solution meets our requirement identifying any areas where it does not meet this strategic goal.		
We confirm that in compliance with this requirement, we have detailed below how our solution meets the requirement identifying areas where it does not meet the Buyer's strategic goal. Our solution, based on the existing applications to provide minimum risk and maximum continuity for users, also partly meets other the remaining aspects of the Non-Functional Requirement for Browser Compatibility. This will be the case for the Viable Product Release and for the Operational Service Commencement Date. Atos is pleased to advise that the newer elements of its solution have been built using HTML5 to allow for rich, engaging services and content without the need for additional plugins or installed software. Most importantly, the Assessment Tool functionality, as used by HPs to construct assessment reports, was built relatively recently using HTML5. This offers users various other benefits, such as offline application cache, and results in much cleaner, simplified code, which will streamline the development process for future work. In particular, this offline application cache provides proven and seamless business continuity in the event of interruptions in connectivity whilst a consultation with the claimant is in progress. Atos confirms that in areas of new development, where practical, HTML5 will be used and client-side scripting will be avoided, to produce services that are browser, platform, and device agnostic. This may not necessarily be the case with minor amendments to existing screens, as that may require disproportionate and unwarranted cost. Other than the Assessment Tool functionality, the majority of components of the existing solution were built on foundations utilising slightly older technologies. For example, PRS was developed using the Java Spring framework with the front-end		

being driven by jQuery. There are also elements of client-side scripting, including JavaScript or Java-based JSPs. The SAMS application, being a configured Siebel implementation, does not offer an HTML5 front end. Nevertheless, the Buyer can be assured that all of these components have thus far proved to be stable, reliable, and readily maintainable, and to date have met usability needs perfectly adequately.

Whilst the upgrading of the full PRS application to HTML5 has not been included within this proposal (as the Buyer may not consider it a worthwhile investment given the impending migration to HAS and decommissioning of the PIP IT systems) we certainly have the capability and expertise to undertake such an upgrade should the Buyer wish to make this further investment. For example, on [redacted] [Redacted FOIA S43 Commercial Interest] Atos used HTML5 in the design and development of the full end-to-end mobile solution for the Tax-Free Childcare service. That solution has been used by 2.3million families/150,000 childcare providers to access services with no quality issues reported relating to access/device compatibility.

In line with Atos's drive to digitise customer systems and service operations, new PIP IT functional requirements will be assessed and, if appropriate, developed on the new Digital Platform (Atos's public cloud hosted environment for secure enterprise consumption of AWS services). Any development on this platform would be built around open web standards, in particular including HTML5.

Fresh Digital Innovation

496 words

4.2r)	GDPR	Weighting 0.30% Aesthetic & Functional Characteristics
Guidance:		
The solution must allow the Buyer to comply with the General Data Protection Regulation (GDPR) legislation that came into effect on 25th May 2018. Further information about compliance can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, describe how your solution (and its supporting people and process elements) deliver the appropriate technical and organisational measures required to meet the requirements of GDRP. This could include, but is not limited to: data retention, archiving, encryption, or anonymisation.		
Introduction Atos confirm that our solution will meet the Requirement for General Data Protection Regulations (GDPR) and will comply with all stipulations of applicable Data Protection law. Our solution will also support Buyer compliance with GDPR. This requirement is met by our current service and, consequently, it will be included for Viable Product Release and Operational Service Commencement Date. GDPR Compliance Atos supports other public and private sector organisations to achieve GDPR compliance and will leverage this expertise to support the Buyer. Our Technical and Organisational Measures to ensure confidentiality, integrity, availability and resilience of processing systems for the protection of data, meet or exceed NCSC requirements. Our solution will enable the Buyer compliance with all GDPR principles for storage, transmission and processing of Personal and Special-Category data, comfortably meeting the NCSC requirements. To achieve low-risk processing of personal data, the following protective measures are followed: • Minimise the amount of personal data • Encrypt data as early as possible • Create transparency regarding procedures and processing of data • Delete or anonymise data as early as possible • Minimise access to data • Pre-set existing configuration options to the most privacy-friendly values • Document the assessment of risks.		

Atos maintains a group-wide programme which ensures that delivery of services to customers complies with GDPR, and within the UK, the Data Protection Act 2018.
Atos will collaborate with the Buyer to ensure compliance with all relevant data protection provisions following the best practice below:

- Establish Data Controller and Data Processor roles and responsibilities
- Detail obligations of Data Controller and Data Processor as they apply to the Buyer's requirements
- Assure adequacy of any proposed processing of Personal Data
- Evidence the adoption of appropriate Technical and Operational Measures to ensure the security of Personal Data
- Agree (with the Buyer) the scope and sensitivity of all Personal data to be processed
- Consider and agree the nature of data processing and compliance requirements of any subcontractors
- Complete any Privacy Impact Assessment or similar documentation.

To support the Buyer to meet the requirements of the GDPR legislation, Atos will identify the data to be stored, determine the need for storage, and only store the minimal amount of data needed for a legitimate purpose and for the appropriate retention period.
Least privilege access will be applied on a need-to-know basis for those who require access or process personal data through well-defined and monitored interfaces.
In line with the requirements documented in the Data Protection Act 2018 and under GDPR, the encryption of personal data is an appropriate and proportionate control for its protection.
We will protect the Buyer's data stored and processed within the public cloud using native Public Cloud encryption for hosting servers. This will protect the Buyer data from unauthorised access by public cloud infrastructure administrators or unauthenticated cloud external attackers.

The Buyer can be assured that one of our key solution themes is operational stability and security. This includes our adherence to GDPR, and our support to enable the Buyer to meet the GDPR requirements.

495 words

4.2s)	Components	Weighting 0.20% Technical Merit
Guidance:		
The Potential Providers technical operators must be able to update and configure components of the solution without impact on other unrelated solution components. Full documentation of all components of the solution must be provided. This requirement is required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)		
Question:		
Incorporating the guidance above, your response should detail how it meets our Components requirement.		

We confirm that our solution fully meets the Non-Functional Requirement for Components, and this will be provided for both Viable Product Release and for the Operational Service Commencement Date.
Component Configuration
Atos confirms that its technical operators will be able to update and configure components of the solution without impact on other unrelated solution components. The solution comprises numerous discrete components, including:
• PRS and SAMS user interfaces and Oracle databases
• PRS and SAMS back-end business service processes
• MIS staging, foundation, analytical and reporting layers
• The jBPM workflow used by PRS
• The Drools rules engine supporting:
  ○ Risk-based audit
  ○ The phrase-builder function
  ○ Initial review triage/segregation
• Bulk print & SMS templates
• Individual interface transaction definitions.
 	
By design, the interdependencies between all of the above have been kept to the minimum necessary in order to address the business needs. Each can be maintained independently of the others such that in many cases (depending on the requirement to be addressed), business changes are implemented in one area with no impact on any other solution components. For example:
• Changes can be made to risk-based audit rules or phrase-builder content/triggers with no application impact
• PRS functional changes can be made with no impact on the database, workflow, interfaces or associated rules engines
• Claimant notification changes can be made without impacting the source systems.		

As would be expected, more significant business changes tend to have an impact across components. For example:

- Support GPFR fee payments will require changes to the PRS application front end and database, MIS (to ingest the new data) and a new interface transaction, but will not impact SAMS, the jBPM workflow, the rules engine nor notifications
- Support for the new IF6 interface will require changes to the workflow (as the 'closure' step will no longer represent a wait state), a new interface transaction triggered automatically by the workflow at appropriate points, but (to be confirmed in detailed design) no impact on any other component.

Component Documentation

Atos confirms that full documentation of all components of the solution will be provided. This will include:

- Overall solution level design
- Architecture design
- PRS and SAMS data models
- PRS and SAMS use case definitions
- PRS workflow definition
- Systems interface definitions
- Printed output/SMS message specifications
- MIS report specifications
- as well as more detailed technical design artifacts.

Many, if not all, of the above have previously been shared with the Buyer in connection with the current PIP contract with IAS. It is these products that will be updated to reflect the new PIP IT service, with all changes from existing versions clearly tracked to provide a clear audit trail and version history.

435 words

4.2t)	Solution Hosting	Weighting 0.20% Technical Merit

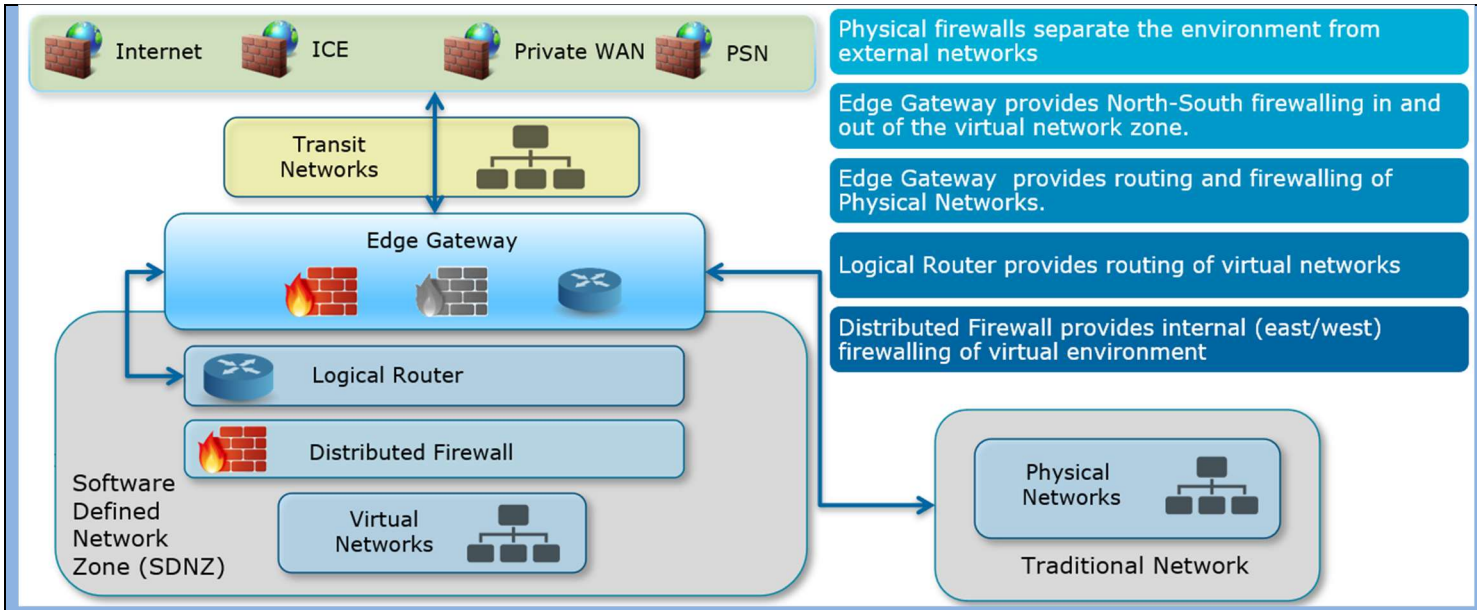
Guidance:

The solution components must be able to be deployed into Buyer Approved Public cloud environments or the Suppliers own hosting environments.
Hosting environments will be provisioned and supported by the Supplier.
This requirement is required for Viable Product Release (See Attachment 6.1)
This requirement is required for Operational Service Commencement Date (See Attachment 6.1)

Question:

Incorporating the guidance above, your response should detail the Solution Hosting componentry and location(s).

Introduction
Our solution fully meets the Requirement for Hosting. Given our solution is predicated on the current services we provide, it will of course be available for the Viable Product Release milestone and the Operational Service Commencement Date.
Hosting Environments
Our solution will be hosted on the Atos IRIS UK Cloud Platform, a multi-tenanted community cloud designed for OFFICIAL / OFFICIAL SENSISTIVE workloads. It currently hosts services connected to national and local government including DWP, [redacted] [Redacted FOIA S43 Commercial Interest].
As our proposed hosting solution is an extension of our current solution enhanced with a new cloud native, digital platform supporting much of the new functional requirements, this approach will assure a quick and safe transition and deliver operational stability and security.
The Platform is delivered from two geographically separate Tier 3 UK Data Centres. Diverse connectivity is available including Private WAN, Internet, PSN and Integrated Cloud Edge, the latter enabling connectivity to Public Cloud for Hybrid Cloud scenarios.
Two availability zones enable active/active, active/passive workloads offering synchronous replication with zero data loss. Storage services include tiered Block and File storage, snapshots and on/off site backups. Network services include Edge Firewalls, Load Balancing, NAT and VPNs. All services are delivered into a customer dedicated software defined network zone depicted below.



The platform is designed to NCSC Cloud Security Principles, builds are hardened to CIS benchmarks and undergo an annual Check ITHC including PSN Assurance and CE+.

The tenant environment consists of three separate zones – Production, Non-Production and Development. They are fully segregated with independent access controls and network segregation including Edge Firewalls. The availability of Integrated Cloud Edge connectivity to public cloud offers the opportunity to leverage public cloud capabilities.

Hosting environment provisioning and support

Provisioning of services is via a front-end https portal whereby a standard set of services can be auto-provisioned.

All Platform administrative support personnel are UK Based and Security Cleared. They hold multiple vendor certifications in the technologies that underpin the platform, including VMware Certified Professional, DellEMC Proven Professional, Juniper Networks Certified Associate, Fortigate Network Security Professional.

Onboarding to IRIS UK is a well-established process. A team including Deployment Manager, Technical Architect and DevOps Engineers provide continued support throughout the deployment and migration process and into operational support.

New functional requirements will be assessed and developed on the appropriate platform, and in line with Atos' drive to digitise our systems and services operations, it is expected that the current delivery team will proactively undertake this effort. The new Digital Platform offers cloud native features such as PaaS Database Services, Containers, Functions and Micro

Services, delivering improved scalability and fast deployment cycles through CI/CD pipeline techniques, in turn leading to improved flexibility and more efficient platform operations.
This approach is fully aligned with the DWP's SRE Dev Ops approach for cloud-native infrastructure and application builds/deployment. Functional modules that have been converted or natively built in the Digital Platform can in turn be more readily re-used in and/or integrated with the DWP's planned HAS platform.

498 words