

4.2u)	Documentation	Weighting 0.10% Technical Merit
Guidance:		
<p>A set of documentation must be provided, that is sufficiently detailed for the Buyer to understand the solution components from a business, security and technical perspective</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should detail what High Level solution documentation will be produced in order to meet the Viable Product Release and the implementation of Operational Services by the required commencement date. Capturing details of the outline purpose and scope of each document.</p>		
<p>Atos will provide the following updated high-level solution documentation to the Buyer and fully meet this Non-Functional Requirement for Relevant Documentation to understand the solution components from a business, security and technical perspective. This documentation will be available for Viable Product Release and by the Operational Service Commencement Date.</p> <p>All high-level solution documentation will adhere to the Atos Unified Engineering Method (UEM), which is a framework of engineering processes, roles, products, and governance covering the entire customer solution lifecycle. UEM provides a unifying framework used to ensure all high-level solution documentation provided is developed, reviewed and approved across technical and solution teams for overall assurance and quality.</p>		

Unified Engineering Method (UEM)

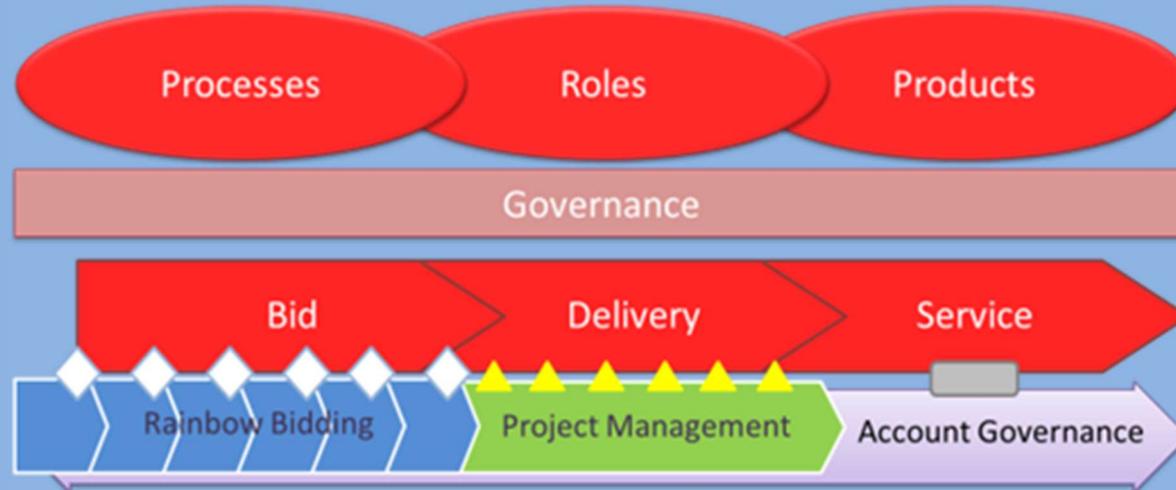


Diagram 1: Atos Unified Engineering Method (UEM)

Technical

- PIP Architecture Baseline
- PIP Architecture Standards
- PIP Architecture Design Decision and Policy Exception Register
- PIP Systems Architecture
- DWP PIP - System maps
- PIP ASC Provisioning Guidelines
- IRIS Sentinel HLD
- IRIS UK Managed IaaS Platform Services HLD
- DWP PIP WAN site details
- DWP PIP Proving HLD
- DWP PIP DataStage & Cognos HLD
- DWP PIP Secure File Transfer
- DWP PIP Bulk Printing
- DWP PIP Oracle Database HLD
- DWP PIP Datastage HLD

- DWP PIP BPS HLD
- DWP PIP SQL Design
- DWP PIP Offline Assessment Tool Architecture
- IF7 and IF8 Integration Architecture
- DWP PIP Application Authentication States
- DWP PIP Account Disaster Recovery Invocation
- DWP PIP Network High Level Design
- DWP PIP Globalscape low level design
- DWP PIP Disaster Recovery HLD.

Business/Service

- PIP Business Architecture
- Cloud Hosting Service Definition – IRIS UK Cloud Hosting
- DWP PIP Operational Level Agreement
- Service Definition – IRIS UK Cloud Hosting
- DWP PIP Operational Level Agreement
- PIP Service Architecture
- DWP PIP IT Service map.

Security

- Government Security Classifications – FAQ Sheet 2: Managing Information Risk at OFFICIAL
- PIP Security Architecture
- Vulnerability Scanning Service HLD
- Proxy Service HLD.

It is Atos' process and standard – and broader best practice – that we complete and deliver these documents across our entire client base, public and private; each document going through a full review and approval process, enabling us to ensure consistency of service. We have adopted a similar structure for DWP, [REDACTED] [Redacted FOIA S43 Commercial Interest]. The benefits to the Buyer are that a number of these design documents are already in place for the current operations and will only need to be reviewed and improved as part of the discovery, initiation and design phases within the transition plan. This means the Buyer will be familiar with existing documentation standards in place. The documentation is of high-quality, consistent, and up to date with latest technology standards, ensuring a high-quality service provision whenever this documentation is used.

432 words

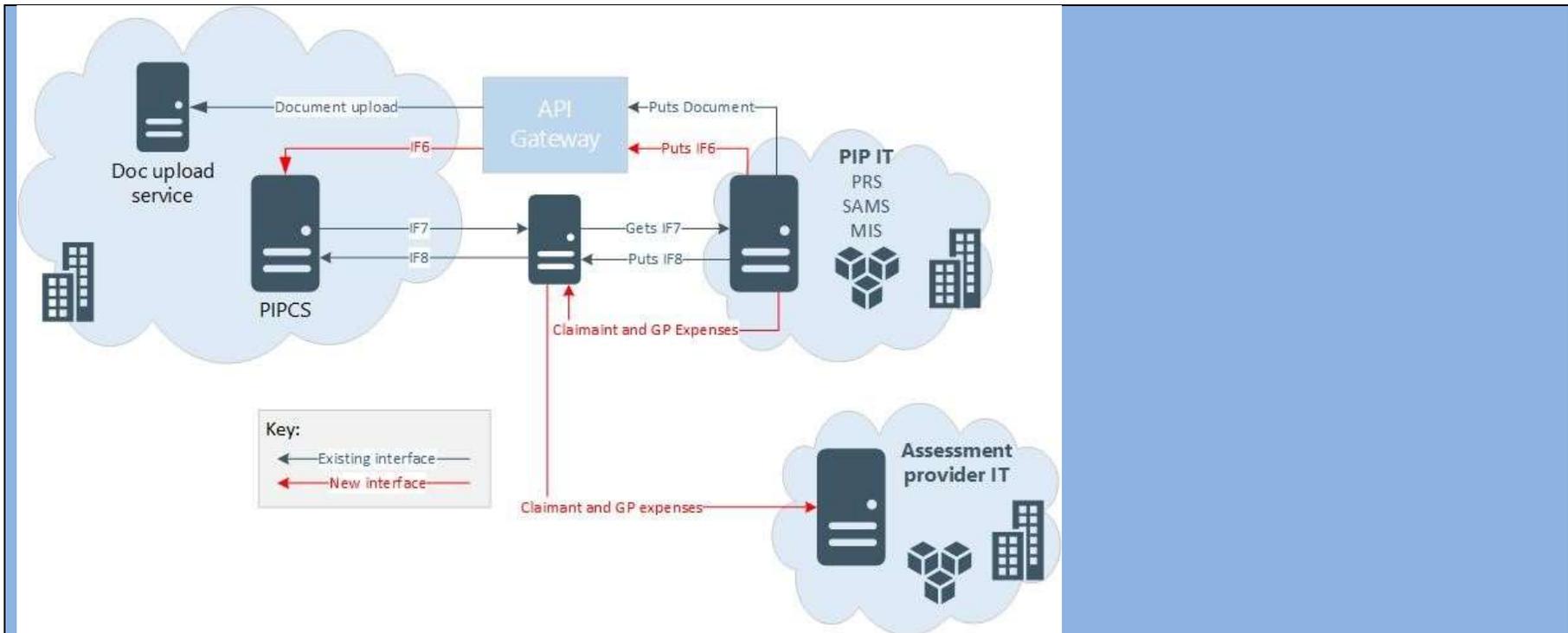


Quickest, safest
transition



Operational stability
and security

4.2v)	Application Programming Interface (API) and Integration	Weighting 0.10% Technical Merit
Guidance:		
<p>Detailed API and Integration documentation, demonstrating how any APIs or integration points within the solution should be used/how they work must be provided. All API integrations with the Buyer systems will be via the API Gateway and must be achieved in a manner conformant with the Buyer's integration specifications.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should include all High Level API and Integration documentation required to meet our requirement</p>		
<p>We confirm that our solution fully meets the requirement for Application Programming Interface (API) and Integration, in particular that all API integrations with the Buyer systems will be via the API Gateway and will be achieved in a manner conformant with the Buyer's integration specifications. This will be included within the Viable Product Release and by the Operational Service Commencement Date.</p> <p>Our API development process will be based on open standards which will allow for secure, simple communication for services between various endpoints. For example, our solution will use RESTful SOAP XML requests to 'GET' and 'POST' data whenever required to provide an efficient means of communication across applications.</p> <p>API and Integration Documentation</p> <p>For all existing and proposed new APIs and integration (including interfaces to Healthcare Provider systems), we will provide thorough documentation to the Buyer, building on the existing documentation provided by Atos in support of the AIS solution. Our objective is to use API documentation tools such as OpenAPI or RESTful API Modelling Language (RAML). This will act as an accurate reference source that describes the API in detail.</p> <p>API Gateway</p> <p>Our solution will implement the Buyer's API gateway and will be fully conformant with the Buyer's integration specifications, to manage the various API services and endpoints being used in the overall solution.</p>		



The solution is able to interface 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 will build upon the existing API gateway endpoints from the Buyer currently provided; we will extend the endpoints and features and will incorporate new APIs into the gateway as required. In particular, the 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. In line with Atos's general drive to digitise our systems and service operations, new functionality that needs to be supported will be assessed and, if appropriate, developed on Atos' Digital Platform. The Digital Platform refers to Atos' public cloud hosted environment for secure enterprise consumption of AWS services. Both the existing solution and the new Digital Platform will be able to communicate via API endpoints, which will ensure complete compatibility across the systems. 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.



483 words

4.2w) Security	Weighting 0.60% Technical Merit
Guidance:	
<p>As the Buyer adopts a 'Public Cloud First' strategy to service, hosting the solution must comply with the Cloud Security Principles published by the National Cyber Security Centre.</p> <p>The 14 Cloud Security Principles can be read at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles</p> <p>The solution should also be compliant with the following NCSC principles:-</p> <p>Zero Trust - https://www.ncsc.gov.uk/blog-post/zero-trust-principles-beta-release</p> <p>Bulk Data Principles - https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main</p> <p>Security Design Principles for Digital Services - https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, in your response, identify which Cloud Security Principles your solution is/is not compliant with.</p>	
<p>Introduction</p> <p>Our solution fully meets the requirements for Security. The foundations to our solution are inherited from our current services supporting PIP, whilst refining and enhancing those capabilities enabling us to meet the Operational Service Commencement Date.</p> <p>NCSC Cloud Security Principles</p> <p>Our solution is a refreshed version of the operational platform supporting the current PIP service and will be hosted on the Atos IRIS Platform.</p> <p>IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads, fully compliant with all 14 NCSC Cloud Security principles.</p> <p><i>Data in Transit</i></p> <p>Is protected using secure Private WAN connections and encrypted VPN connections.</p> <p><i>Asset Protection and Resilience</i></p> <p>IRIS is hosted in accredited Tier-3 datacentres providing the necessary security and resilience. Operational/Live and backup data are stored on separate, enterprise-class, storage arrays employing data-at-rest encryption.</p> <p><i>Separation between Users</i></p>	

IRIS being a multi-tenant platform, Tenant separation is fundamental to its security and is key to all design decisions. Separation is achieved through appropriate network, compute and storage technologies, including virtualisation.

Governance Framework

Technical and Security Governance are fundamental elements of the service. A weekly Technical Design Authority meeting is overseen by the platform Lead Architect and a monthly Security Working Group is overseen by the Operational Security Manager for the Service

Operational Security

The IRIS Platform is subject to a strict change management procedure.

All changes (except pre-approved Standard changes) are subject to Technical, Service and Peer Approvals. All assets are recorded in a secure CMDB

Personnel Security

Administrators of the IRIS Platform and our service staff are all Security Cleared.

Secure Development

Development follows "Security-by-Design" principles. Service designs are reviewed to ensure alignment to the *Open Web Application Security Project (OWASP) Secure Coding Practices* and alignment to the NCSC Security Design Principles

Supply Chain Security

Atos assesses all suppliers who provide equipment, hardware or software, as part of the procurement process.

Secure User Management

Strict user separation is maintained between IRIS Platform Management and Tenant Management.

Identity and Authentication

Strong authentication is enforced for platform and tenant administrators using two factor authentication and dedicated encrypted management connections.

External Interface Protection

All external connections are protected by Intrusion Protection Services.

Internet connectivity is protected by a DDOS protection service.

Secure Service Administration

Administration is via Bastion Hosts. Connectivity is via a dedicated end-to-end encrypted channel.

Audit Information for Users

Access to the service is audited. Audit logs are reviewed by the Operational Security Manager and available upon request.

Secure Use of Service

The Atos Secure Use of Service policy dictates the use of services on the IRIS platform.

Zero Trust Compliance

The solution is compliant with the NCSC Zero Trust principles utilising micro-segmentation within the architecture.

Bulk Data Principles Compliance

The solution utilises Technical and Organisational Measures that meet the NCSC requirements for the protection of data. Security Design Principles for Digital Services Compliance
The solution is compliant with all NCSC Security Design Principles.



Operational stability
and security

491 words

4.2x)	Data protection and information security for Buyer provider	Weighting 0.40% Technical Merit
Guidance:		
<p>All Potential Providers of services to the Buyer must comply, and be able to demonstrate compliance, with the relevant policies and standards. These are listed within the link below. https://www.gov.uk/government/publications/data-protection-and-security-of-information-supplying-to-Authority 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)</p>		
Question:		
Incorporating the guidance above, in your response, identify which policies and standards your solution is/is not compliant with.		
<p>Introduction Our solution is fully compliant with the Buyer’s security policies and standards and utilises currently provided capabilities as a foundation, to be refined and enhanced as appropriate in meeting additional requirements. This minimises development and underpins our assurance of making the required capabilities available for the Viable Product Release and the Operational Service Commencement Date. Data protection and Information Security Our proposed solution will be hosted on the IRIS UK Cloud Platform.</p>		

IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official/Official Sensitive workloads for which a comprehensive suite of Atos security-related policies and standards already exist.

The suite of IRIS UK security policies and standards meet, or exceed, the requirements of the Buyer’s procurement security policies and standards.

The IRIS UK Platform operates its own Security Working Group (SWG) chaired by a UK based Operational Security Manager. At each meeting, an operational security report is presented covering security-related topics including security compliance, patching and antivirus status, security incidents, security deltas, security exceptions, security vulnerabilities and threat updates.

The SWG will also provide ongoing monitoring of our compliance with applicable security policies and standards.

The following table identifies which policies our IRIS platform is compliant with.

(1) Policy	(2) Relevant to our solution?	(3) Is our solution Compliant?
(4) Acceptable Use Policy	(5) Yes	(6) Yes
(7) Information Management Policy	(8) Yes	(9) Yes
(10) Personnel Security Policy	(11) Yes	(12) Yes
(13) Physical Security Policy	(14) Yes	(15) Yes
(16) Cryptographic Key Management Policy	(17) Yes	(18) Yes
(19) Email Policy	(20) Yes	(21) Yes
(22) Forensic Readiness Policy	(23) Yes	(24) Yes
(25) Microsoft Teams Recording and Transcription Policy	(26) Yes	(27) Yes
(28) Privileged Users Security Policy	(29) Yes	(30) Yes
(31) Remote working security Policy	(32) Yes	(33) Yes
(34) Security Classification Policy	(35) Yes	(36) Yes
(37) SMS Text Policy	(38) Yes	(39) Yes
(40) Social Media Policy	(41) No	(42) Yes
(43) Technical Vulnerability Management Policy	(44) Yes	(45) Yes
(46) User Access Control Policy	(47) Yes	(48) Yes
(49) Common Standards for Identity Verification and Authentication (CSIVA) of DWP customers	(50) Yes	(51) Yes

Schedule 1	Access and Authentication Controls SS-001 (part 1)	(52)	Yes	(53)	Yes
Schedule 2	Privileged User Access Controls SS-001 (part 2)	(54)	Yes	(55)	Yes
Schedule 3	Public Key Infrastructure & Key Management (SS-002)	(56)	Yes	(57)	Yes
Schedule 4	Software Development (SS-003)	(58)	Yes	(59)	Yes
Schedule 5	Database Management System Security Standard (SS-005)	(60)	Yes	(61)	Yes
Schedule 6	Security Boundaries (SS-006)	(62)	Yes	(63)	Yes
Schedule 7	Use of Cryptography (SS-007)	(64)	Yes	(65)	Yes
Schedule 8	Server Operating System (SS-008)	(66)	Yes	(67)	Yes
Schedule 9	Hypervisor (SS-009)	(68)	Yes	(69)	Yes
Schedule 10	Desktop Operating System (SS-010)	(70)	Yes	(71)	Yes
Schedule 11	Containerisation (SS-011)	(72)	Yes	(73)	Yes
Schedule 12	Protective Monitoring Standard - For External Use (SS-012)	(74)	Yes	(75)	Yes
Schedule 13	Firewall Security (SS-013)	(76)	Yes	(77)	Yes
Schedule 14	Security Incident Management (SS-014)	(78)	Yes	(79)	Yes
Schedule 15	Malware Protection (SS-015)	(80)	Yes	(81)	Yes

Schedule 16Remote Access (SS-016)	(82) Yes	(83) Yes
Schedule 17Mobile Device (SS-017)	(84) No	(85) Yes
Schedule 18Network Security Design (SS-018)	(86) Yes	(87) Yes
Schedule 19Wireless Network (SS-019)	(88) No	(89) Yes
Schedule 20Voice & Video Communications (SS-022)	(90) No	(91) Yes
Schedule 21Cloud Computing (SS-023)	(92) Yes	(93) Yes
Schedule 22Virtualisation (SS-025)	(94) Yes	(95) Yes
Schedule 23Application Security Testing (SS-027)	(96) Yes	(97) Yes
Schedule 24Microservices Architecture (SS-028)	(98) Yes	(99) Yes
Schedule 25Securely Serving Web Content (SS-029)	(100) Yes	(101) Yes
Schedule 26Oracle Database Security (SS-030)	(102) Yes	(103) Yes
Schedule 27Domain Management (SS-031)	(104) No	(105) Yes
Schedule 28Security Patching (SS-033)	(106) Yes	(107) Yes



Operational stability
and security

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

498 words

4.2y)	Data integrity	Weighting 0.20% Technical Merit
Guidance:		
<p>The solution must maintain end-to-end integrity of all data at all times. All processing whether through batch processes, real-time using API or performed by user/administrative interface, must adhere to the characteristics of Atomicity, Consistency, Isolation and Durability (ACID test). 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)</p>		
Question:		
Incorporating the guidance above, your response should include details about Data Integrity of your solution		
<p>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 the Viable Product Release and by the Operational Service Commencement Date. Our proposed solution stores all persistent data in either Oracle or relational SQL databases to ensure the end-to-end maintenance of data accuracy and consistency at all times. Transactions written to the databases, either via applications, batch processes or inter-system communications, use industry standard drivers to ensure transactions happen in an atomic, consistent, isolated and durable manner, provided by the SQL databases inbuilt locking, commit and rollback mechanisms. The solution maintains a separation of concerns in terms of data storage and integrity related to different functions. This is based, on the sensitivity of data as well as who the intended end-users are, for example separate database storage is provided for:</p> <ol style="list-style-type: none"> 1. Identity & Access management for RBAC of the various components 2. Patient assessments by Health Professionals using the Patient Referral System (PRS) 3. Appointment bookings and management by Agents using the Siebel Appointment Management System (SAMS) 4. Bank payment of expenses to PIP clients 5. Management Information to produce necessary reporting for SLA and KPI compliance. <p>Data integrity is also supported by:</p> <ol style="list-style-type: none"> a. Using constraints to enforce business rules and ensure values are unique and/or not null where required b. Enforcing business rules and/or valid values with application code c. A comprehensive, automatically generated, audit trail system to provide the 'breadcrumbs' to accurately pinpoint the source of a problem d. Regular backups of all databases 		

e. Geo-resilient disaster recovery.

Examples of maintaining data integrity include:

- Batch processing of tasks, referral cases and any changes in circumstances from The Buyer's PIPCS will undergo input validation and ensure data has not been corrupted before processing
- Integrity of individual database transactions is extended into the bespoke PRS application code to ensure all related functional transactions are completed correctly or not at all
- When an end-user commits changes within the PRS application this may trigger back-end activities such as workflow progression, invocation of the rules engine and/or sending of data to the SAMS scheduling application. Transaction management is in place such that if any of these downstream actions fail then an error message will be displayed to the end-user and the entire transaction is rolled back.

In the event of data migration from a third party, data Integrity and no-data loss are the primary focus of migration testing. This consists of validating the data between the source and target and verifying the data in destination system. Ensuring that the migrated data on the target system is exactly same as the source is the key objective of migration testing. Automated data validation of data volumes, data content, data integrity, identification of missing data and duplicate records will be performed using Atos's Data Validator Tool.



Operational stability
and security

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

494 words

4.2z)	Scalability	Weighting 0.30% Technical Merit
Guidance:		
<p>The solution must have a documented scaling process that can be implemented on a cloud-hosted or Potential Provider hosted platform. Documentation must state how to scale (including support for automatic scaling) across different parts of the solution (database, application servers, web servers, etc.) to meet the volumetric information detailed in the overall document. Factors affecting the solution’s response time sensitivity must be clearly identified.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is not required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
Incorporating the guidance above, in your response describe how your Solution can scale to meet our requirements.		
<p>Introduction We confirm that our solution fully meets the requirement for Scalability and that as this requirement is already available for the current service, it will be included for Viable Product Release and the Operational Services Commencement Data.</p> <p>Scalability Our solution, hosted on the IRIS UK Cloud Platform has horizontal and vertical scalability available to tenants to allow workloads to ‘flex’ up or down as required by the application and the business. This is the same platform on which the current AIS service is hosted and the Buyer will be aware that it is fully scalable. New functional requirements will be delivered from the New Digital Platform which brings additional scalability features.</p> <p>Scalability of network bandwidth, storage and compute are all key features of the platform and regularly leveraged by tenants. Scalability is managed by Atos via the IRIS UK Retina Portal.</p> <p>Scale up enables the addition of resources to the systems delivering the service include web, application and database. This is delivered via a front-end portal request in response to observed usage either by utilisation reporting from monitoring tooling or an automatic alert when a workload threshold is met. Requests for a scale up of resource is automatically provisioned by the platform.</p> <p>Scale out enables additional nodes to be added to cope with additional workload. This may be in response to automatic alerts or observed usage over time through performance reporting.</p> <p>The scaling requirement is supported by monitoring tools including Oracle Cloud Control, JBoss Operations Network and Systems Centre Operation Manager.</p> <p>Where customer workloads have been ‘over-sized’ workloads can be scaled down or scaled in to reduce cost and avoid wasted resources. This functionality is also leveraged during tenant off-boarding, allowing a gradual draw down of resource and associated cost.</p>		

The platform is proactively capacity managed by Atos UK Cloud Enterprise Solutions and expanded on a regular basis to ensure no scaling limits are reached by tenants. As today, a monthly capacity meeting of key stakeholders will take place to review current capacity against short, medium and long-term forecasts with a weekly capacity review taking place with a smaller cohort. New functional requirements will be delivered on the Digital Platform, which brings with it, additional scalability improvements including auto-scaling in response to utilisation or throughput thresholds, as well as setting up scaling plans optimised for availability and/or cost for most platform resource sets.

Where possible, serverless architectures will be employed to avoid having to manage or even configure automatic capacity scaling (and/or de-scaling; these techniques work in both directions). In line with Atos' general drive to digitise our systems and service operations, the current delivery team has already begun to convert our existing platform into a digital one, to:

1. Increase the efficiency of the Health Professionals and the Buyer's internal users of the platform
2. To lower on-going operations cost
3. Refactor current functionality to micro-services, to ease migration and/or integration with the Buyer's planned HAS platform.



489 words

4.2aa)	Capacity	Weighting 0.30% Technical Merit
Guidance:		
<p>The solution must be capable of supporting the documented number of concurrent agent user accesses and processing the forecast business volumes while still meeting the functional, non-functional and operational requirements. 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)</p>		
Question:		

Incorporating the guidance above, in your response describe how your Solution can meet our capacity requirements, any constraints for meeting the requirements should be identified.

Introduction

Our solution is fully capable of supporting the documented number of concurrent agent user accesses, and processing the forecast business volumes, whilst still meeting the functional, non-functional and operational requirements. Our solution is founded on our current tried and tested systems, so will be included for Viable Product Release and the Operational Service Commencement Date.

Scalability\Capacity

Our solution is hosted on the IRIS UK Cloud Platform, our UK Government Secure multi-tenanted Cloud platform. We proactively manage capacity on this platform to fulfil the scalability requirements of our tenants. This is the same platform on which the current IAS service is hosted and it is truly scalable, as the Buyer should already be aware.

As today, a monthly capacity meeting of key stakeholders will take place to review current capacity against short, medium and long-term forecasts with a weekly capacity review taking place with a smaller cohort. The platform has undergone many incremental capacity upgrades since its inception and a smaller number of major upgrades.

The Compute, Storage and Network components are built with enterprise class processing equipment with built in redundancy at all layers. Delivering infrastructure that solutions can leverage to achieve rapid response times of the most demanding applications and databases. The architecture is modular such that capacity can be scaled with relative ease.

Tenants of the IRIS UK Cloud Platform, including the solution proposed for delivery of the proposed PIP IT service can scale up and/or down capacity as required by the business. Our solution offers gradual scaling as services are on-boarded or offboarded. Capacity is scaled dynamically by the Atos delivery team via the IRIS UK Retina Self-Service HTTPS Portal.

Atos will work with the Buyer and standardise the on-demand and automated allocation of compute resources in the cloud environment using templates and scalesets. We will use virtual machine (VM) scaling to automatically create and manage a group of identical and load balanced VMs. The number of VM instances will automatically increase or decrease in response to demand (auto-scale) or a defined schedule. Scaling will also provide High Availability (HA) to applications and allow central management, configuration and updating of multiple VMs.

The Buyer will realise the following benefits:

- Easy to create and manage multiple VMs – VM instances are created from the same base OS image and configuration which increases speed and agility
- Provides HA and application resiliency
- Allows the applications to automatically scale and reduce as resource demand changes – can automatically increase the number of VM instances as application demand increases and automatically reduce the number of VM instances as demand decreases, maintaining response times

-
- Works at large-scale – auto scale means that planned and unplanned peaks and troughs in demand are automatically adjusted for, contributing to application availability, reducing the need for scheduled changes and keeping hosting costs low within Atos' IRIS Cloud Platform.



Operational stability
and security

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

495 words

4.2ab)	Real Time / Batch Processing	Weighting 0.10% Technical Merit
Guidance:		
<p>The solution must provide capability for the Suppliers technical support teams to schedule any necessary batch, or initiate real-time processing without affecting the functionality or availability of the live services.</p> <p>Note: Any real-time or daily batch processing could run concurrently with the service.</p> <p>There must also be an option for additional processing to be scheduled if required, without hindering the performance of the system.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
Incorporating the guidance above, in your response please describe your solution's processing characteristics.		
<p>We confirm that our solution fully meets the Non-Functional Requirement for Real Time / Batch Processing and that as this requirement is already available for the current service, it will be included for Viable Product Release and Operational Service Commencement Date.</p> <p>The proposed solution provides a number of key batch processes which include:</p> <ul style="list-style-type: none"> • Ingestion of referral data • Change of circumstances data • and the exchange of tasks. <p>As well as the following downstream batch processes:</p> <ul style="list-style-type: none"> • Expense payments • Printing of appointment letters and Further Medical Evidence (FME) requests • Creation of MIS reports. <p>Downstream batch processing will take place through Globalscape EFT (Enhanced File Transfer) software which provides a user-friendly managed file transfer capability to support scheduled automation as well as monitoring of folders without scripting for real-time batch processing.</p> <p>Therefore, technical support teams will be able to schedule any necessary batch or initiate real-time processing without affecting the functionality or availability of the live services.</p> <p>Where possible, batches will target 'batch windows' which will align with less-intensive online activity to minimise any potential impact on the performance of the system.</p> <p>With regards upstream batch processing, specifically Interface File Definition IF7, a scheduled file will be processed overnight for the bulk of the data according to the defined process. However, there will be provision in place to support frequent daily batch</p>		

files of smaller volumes containing urgent referral data and/or tasks which will run concurrently with the service without negatively hindering its performance. This real-time batch processing will occur automatically through folder monitoring or can take place on a manual basis where additional processing of files has been requested.

Based on inherent data integrity principles of the application and its relational SQL databases to lock, apply constraints and store information, batch processing can safely be performed during working hours without impacting user functionality and system performance.

All batch processing jobs will be monitored by Atos operational support staff to ensure jobs complete successfully and issues are identified which may result in technical support teams re-requesting or re-issuing the batch file or performing other adjustments to ensure jobs complete successfully.



Operational stability
and security

The Buyer can be assured that one of the key themes of our solution is operational stability and security and our proposed continuation and enhancement of the current solution will ensure continuity of Real Time / Batch Processing.

390 words

4.2ac)	Accessibility	Weighting 0.10% Technical Merit
Guidance:		
<p>The Buyer is required by the Equality Act 2010 to ensure that our applications do not present a barrier to staff with disabilities. To do this we have adopted the European Standard EN301 549 and WCAG 2.1</p> <p>The Solution will need to meet the standards set out above. High level guidance is provided at the following link Understanding WCAG 2.1 - Service Manual - GOV.UK (www.gov.uk) and here EN 301 549 - Accessibility requirements for ICT products and services - DWP Accessibility Manual. The Solution should also be tested against the assistive software solutions used by the Buyer at the latest version in use: Dragon Naturally Speaking, JAWS, Read & Write Gold, and Zoomtext.</p> <p>In response to this requirement, also complete the Accessibility Standards Checklist (included in Annex A to Attachment 6.2)</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should include all High Level solution documentation required to meet our requirement, and in addition complete the Accessibility Standards Checklist (included in Annex A to Attachment 6.2).</p>		
<p>We confirm that our solution meets the requirement for Accessibility and will be included for Viable Product Release and Operational Service Commencement Date.</p> <p>Atos is an advocate and thought leader in accessibility standards and has extensive experience in delivering client digital systems meeting accessibility standards through rigorous testing.</p> <p>Atos has a track record of developing and delivering user-centred simple/accessible services.</p> <ul style="list-style-type: none"> • Atos delivered an employee launchpad portal for the BBC. Accessibility testing compliant with UK Government regulations (GDS) was integral to our approach with WCAG 2.0 AA compliance testing using PA11Y/Axe.JS/JAWS/ZoomText/Dragon, enabling the solution to accommodate those with varying abilities • For the [Redacted FOIA S43 Commercial Interest] service, Atos created user groups targeting key accessibility areas. This service passed GDS Alpha in 2019 as well as achieving compliancy with WCAG 2.1 to AA standards. <p>As a partner of the Business Disability Forum (BDF), Atos contributes to the BDF Assistive Technology Task Force, with experts contributing to policy forums, international standards and an online community called AXSChat (http://www.axschat.com/) to help improve the use of inclusive design and accessible technology.</p> <p>The proposed solution will conform to level AA of WCAG 2.1 ensuring compliance with regulation EN 301 549. The four basic WACG design principles (Perceivable, Operable, Understandable, Robust) will test that the application can support users with accessibility requirements in terms of vision, hearing, mobility as well as thinking and understanding.</p>		

Any system user with accessibility requirements, as determined by and notified to us by the Buyer or FAS Supplier, is taken through a workplace assessment service to correctly determine their needs.

If the workplace assessment identifies requirements for functionality not currently provided by the system, then new functionality will be developed, and user experience testing will be conducted including tests for usability and accessibility.

A dedicated IT function will install the required software such as JAWS, ZoomText and/or Dragon Natural Speaking, onto the user's device(s) and thoroughly test the applications in conjunction with the screen readers, magnifiers and speech recognitions systems before handing the equipment back to the user.

Accessibility testing encompasses various tests including, but not limited to, tests for users with impaired vision, deafness and dyslexia. This testing verifies the usability of the system against the required WCAG 2.1 up to level AA standard mentioned in this non-functional requirement.

The tests will exercise the useability of the system from the perspective of users with varying levels of ability focusing on factors like hearing, sight, colour blindness, dyslexia and keyboard-only users.

The following activities for accessibility testing are performed by a skilled, dedicated team at the beginning of a test cycle:

- Define the evaluation scope (level of adherence, environment, entire application or modules etc.)
- Explore target modules/components and select a representative sample (which pages will be evaluated?)
- Audit the selected sample (evaluate using tools, assistive technology and manually)
- Report/document the evaluation findings.



Improve user and
citizen experience

The Buyer can be assured that one of the key themes of our solution is to improve user and citizen experience and our focus on accessibility fully supports this objective.

499 words

4.3 Non-Functional Requirements (Information Requirements) – 7.50%

The Non-Functional Requirements (Information Requirements) of the Buyer are listed in questions 4.3 below.

For each of the Non-Functional Requirements (Information 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 22.16.2 for the Non-Functional requirements (Information Requirements) detailed evaluation information including the marking scheme used for all of the questions in this section.

4.3a) Architecture	Weighting 0.20% Technical Merit
Guidance:	
<p>Provide appropriate text and/or diagrams detailing infrastructure components (e.g. operating systems, Hosting platforms), discrete technical components (e.g. case management, rules engine, etc.), database, web servers and any third party or COTS software comprising your solution.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail how this requirement can be met. This could be in the format of text or a diagram. What are the technology related architectural requirements of your hosted solution?</p>	
<p>We confirm that our solution fully meets the Requirement for architecture, and that this will be fully established within the Viable Product Release and by the Operational Service Commencement Date.</p> <p>Solution</p> <p>Our proposed solution is a refreshed version of our current platform enhanced with a new digital platform. This approach will assure a quick and safe transition and deliver operational stability and security. The Digital Platform refers to Atos' private cloud hosted environment for secure enterprise consumption of AWS services, and has the potential to support the Buyer's development of the future HAS platform by showcasing the vision for a fully cloud native application infrastructure. New functional requirements will, if appropriate, be developed on this platform in line with Atos' drive to digitise our systems and service operations.</p> <p>Architecture</p> <p>The Architecture solution will comprise of the following:</p> <p>Networking connectivity</p> <p>Networking architecture will continue the current mode of operation, with both internet links into the Atos datacenter, and the PIP WAN interface ingress. The Buyer provided, end user compute (EUC) will access the Atos environment via a Zscaler VPN solution, and Atos will facilitate this access into the PIP-IT infrastructure.</p> <p>End user compute platform</p> <p>Atos will work with the buyer to design, plan and implement any interface points to facilitate connectivity into the Atos PIP-IT platform at the datacenters. The migration plan will deliver these interfaces and any training needed to support access into the system.</p>	

Our solution fully aligns to your plan for EUC and Zscaler delivery, but we appreciate that sometimes issues happen, so in the event of delays, Atos propose a workaround to mitigate any risk with this EUC delivery. If required, Atos will stand up an interim Citrix gateway solution which can facilitate entry from all assessment providers into our infrastructure. The EUC platform only needs to have the Citrix workspace connector installed to allow entry to this Citrix platform and this can be installed on a solution agnostic device. We have successfully implemented such a solution like this for clients including UCLH.

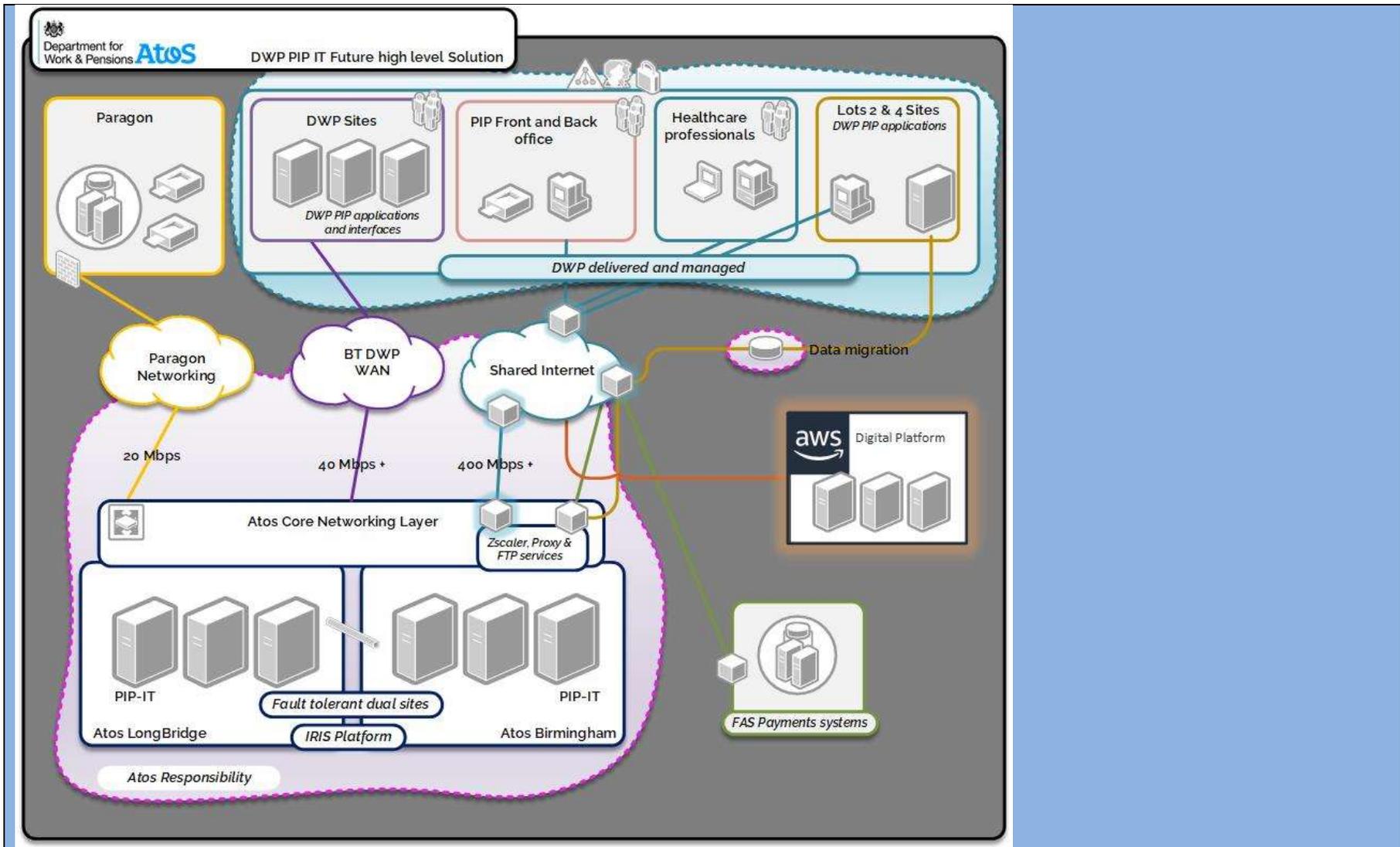
Core application platform

The proposed private secure cloud core application platform comprising of PRS, SAMS and MIS will continue to be hosted on the Atos IRIS infrastructure utilizing COTS products of Redhat for OS and Web services, Cognos, Oracle and Siebel for application reporting and database.

External connectivity

This will remain the same for Paragon links for bulk printing and SMS. Atos will introduce connections for FAS payment systems and migration for Lots 2 & 4.

Contextual Architecture diagram



Future mode of operation high level diagram

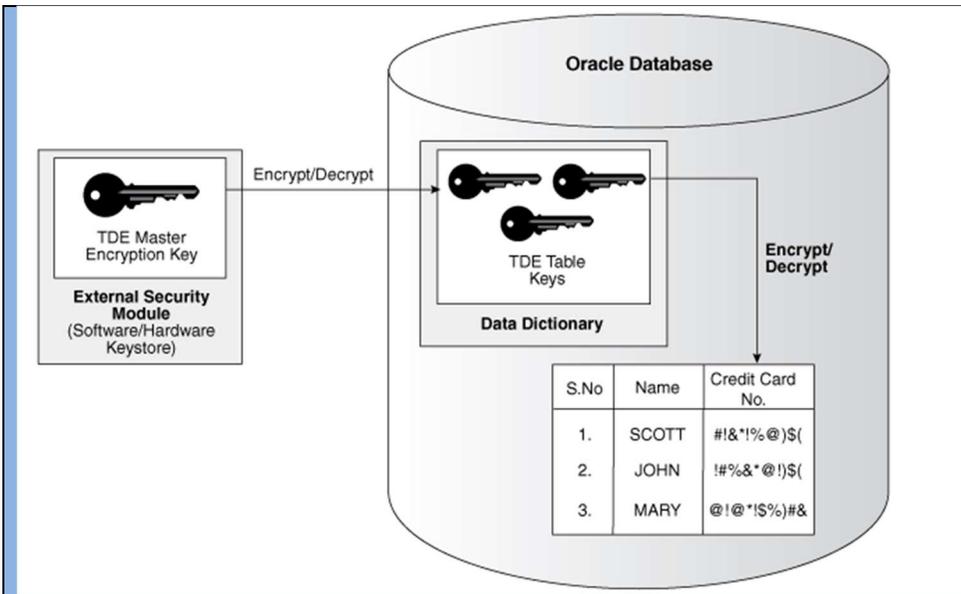
Benefits

The benefit of this solution is a sustainable platform, based on a tried and trusted Atos Infrastructure as a Service. As there is no significant change to the current operations, development activities and account team functions will continue to run with minimal disruption. A major part of the Buyer's user base will continue to access the same system, minimizing the need for any extra training and creating a near seamless transition on the back-end application.



498 words

4.3b) Database Architecture	Weighting 0.20% Technical Merit
Guidance:	
<p>Provide information that explains how your solution can support Encryption of data at rest in relation to Database and file storage technologies.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail how this requirement can be met. This could be in the format of text or a diagram.</p>	
<p>Compliance</p> <p>We confirm that our solution fully meets the requirement for Database Architecture and the encryption of data at rest. Our solution is founded on the service already provided today, which incorporates this capability, and so the requirement will be included for Viable Product Release and by the Operational Service Commencement Date.</p> <p>Data Encryption at rest for Oracle Database</p> <p>Atos is using an Oracle database to store data on the Practitioner Referral System (PRS) and Siebel Appointment Manager (SAMS) systems. The Oracle database has the functionality to encrypt data using Transparent Data Encryption (TDE). Atos has utilised this with other clients including International Airlines Group</p> <p>TDE allows sensitive data to be encrypted and can be applied to individual columns or entire tablespaces. At the column level, data is encrypted using selected table columns. TDE tablespace encryption enables all the data that is stored in a tablespace to be encrypted.</p> <ul style="list-style-type: none"> Once encrypted the data is transparently decrypted for authorized users who have been granted administrative privilege, or applications accessing the data. To prevent unauthorized decryption, TDE stores the encryption keys in a keystore externally to the database. <p><i>TDE Column Encryption Overview</i></p>	



Benefits are as follows:

- Sensitive data is encrypted and therefore safe if the storage media or data file is stolen
- TDE helps you address security-related regulatory compliance issues
- There is no need to create auxiliary tables, triggers, or views to decrypt data for the authorized user or application
- Data is transparently decrypted for database users and applications accessing this data. Database users and applications do not need to be aware that the data is stored in encrypted form
- Data can be encrypted with zero downtime on production systems by using online table redefinition or be encrypted offline during maintenance periods
- There is no need to modify applications to handle the encrypted data, this is managed by the database
- Oracle Database automates TDE master encryption key and keystore management operations.

Data Encryption at rest for File Storage

Atos provides data at rest storage encryption on its IRIS UK environment, used for government projects such as this at DWP and [Redacted FOIA S43 Commercial Interest].

For file storage Data at Rest Encryption (D@RE) will be used to provide hardware-based, on-array, back-end encryption to protect the data from unauthorized access.

D@RE uses the following components:

- Dell EMC Key Trust Platform (KTP) (embedded): This component adds embedded key management functionality

-
- Lockbox: Hardware and software-specific encrypted repository that securely stores passwords and other sensitive key manager configuration information.

Files are passed through the Data Reduction hardware before being sent through the encryption hardware. Data is compressed, deduped, or both before being encrypted by the D@RE process.

The keystore file is encrypted with a 256-bit AES key derived from a randomly generated password file. Keys are self-managed (e.g. no user has access), so there is no need to replicate keys across volume snapshots or remote sites.



Operational stability
and security

485 words

4.3c) Hosting	Weighting 0.30% Technical Merit
Guidance:	
<p>When determining the hosting method for the solution, the Buyer will consider deployment within public hyper-scale cloud or within the Potential Providers hosted environment.</p> <p>Describe how, if supported, your solution can make use of cloud-native services.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail the hosting approach and include, if appropriate, how your solution can make use of cloud-native services.</p>	
<p>Introduction</p> <p>Our solution fully meets the requirement for Hosting services, and as this is already in place as part of our current services to the Buyer it will be included for Viable Product Release and the Operational Service Commencement Date.</p> <p>Hosting Approach</p> <p>Our solution will be hosted on the IRIS UK Cloud Platform which is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads. This public cloud-connected platform already hosts numerous services connecting national and local government including [Redacted FOIA S43 Commercial Interest] [The platform and the Atos Cloud Enterprise Solutions team have a proven track record of delivery of 24 x 7 x 365 services.</p> <p>It offers similar IaaS services to those available from Public Cloud providers such as AWS, including a self-service portal for automated provisioning of available services, provisioned securely and interconnected with the public cloud.</p> <p>There are three environments in support of the solution hosted on IRIS UK:</p> <ol style="list-style-type: none"> 1. Pre-production: true live-like multi-tenant env. used to test all code and changes prior to their implementation in production 2. Production: hosts production application services 3. Disaster recovery: geo-resilient DR solution which can support the Atos PIP solution in the event of a catastrophic failure of the primary data centre. <p>The following services will be provided by the hosting platform:</p> <ul style="list-style-type: none"> • Virtual server compute resources, including support, monitoring & management of the Operating Systems • Block, File and Backup Storage • Data Centre networking, including firewall, load balancing, NAT 	

- Third party connectivity, for example:
 - DWP
 - Paragon for printing and posting appointment, notification and FME request correspondence
 - BPS for secure bank payments of PIP client expenses
- High Availability and Disaster Recovery
- Security including SIEM, Two-Factor Authentication, Intrusion Prevention and DDoS Protection.

Cloud Native Services

New functionality that needs to be supported will be assessed and, if appropriate, developed on Atos' Digital Platform in line with our drive to digitalise customer systems and service operations. In some cases, this has already been proactively undertaken, for example:

1. Functionality that allows machine reading of Further Medical Evidence attached to claims, providing an enhanced and streamlined application to help Health Professionals (HPs) better navigate and work through all referred claims. This new functionality will allow HPs to be more efficient, thus providing a shared saving to both the Buyer and Atos
2. Use of in-built, cloud geo-resilience and auto-scaling as well as PaaS and SaaS leading to:
 - a. More efficient platform operations / lower costs
 - b. Conversion of some functional modules into micro services-based applications, which in turn can be re-used within the Buyer's planned HAS platform
 - c. More streamlined Full Stack Engineering design and delivery techniques including CI/CD pipeline to facilitate state-of-the art configuration management and automated testing.

This approach is aligned with the Buyer's SRE Dev Ops approach for cloud-native infrastructure and application build and deploy.



486 words

4.3d)	Availability	Weighting 0.40% Technical Merit
Guidance:		
<p>The solution must support an availability of 99.9%. (Maximum of 8.76 hours of unscheduled downtime per year). The solution application components need to adhere to a fault-tolerant architecture. All components must be deployable in a highly available mode and protect the end-to-end solution from faults in the underlying hosting infrastructure through built-in resilience with no single points of failure. This requirement is not required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, in your response provide appropriate text and/or diagrams describing any specific architectural design requirements for the solution to meet this non-functional requirement.</p>		
<p>Introduction We confirm our solution fully meets the requirement for Availability as detailed in the requirement specification of 99.9% (maximum of 8.76 hours of unscheduled downtime per year, and that as this requirement is already available for the current service, it will be included for Viable Product Release and the Operational Service Commencement Date.</p> <p>Fault Tolerant Architecture Our solution will be hosted on the IRIS UK Cloud Platform, our UK Government Secure multi-tenanted Cloud supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads. IRIS UK is designed for high availability with multiple levels of redundancy built into every layer ensuring no single point of failure, delivering an availability of 99.9%, achieved in every year of service to date. 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 diagram below provides a high-level view of Compute and Storage Redundancy.</p>		

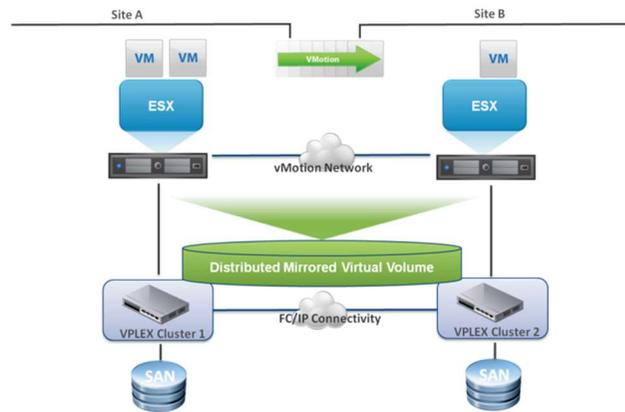
The IRIS UK Platform is hosted in two data centres within synchronous replication distance.

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

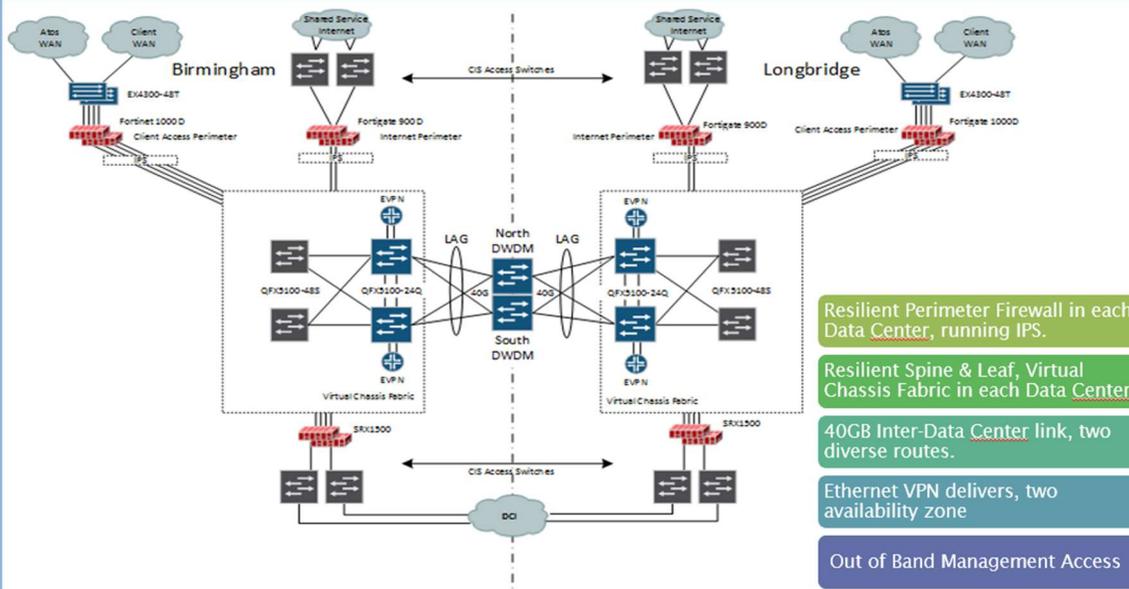
Synchronous SAN storage replication with ability for simultaneous read/write at both data centres.

Latest VMware compute virtualisation software.

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



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.



Resilient Perimeter Firewall in each Data Center, running IPS.

Resilient Spine & Leaf, Virtual Chassis Fabric in each Data Center.

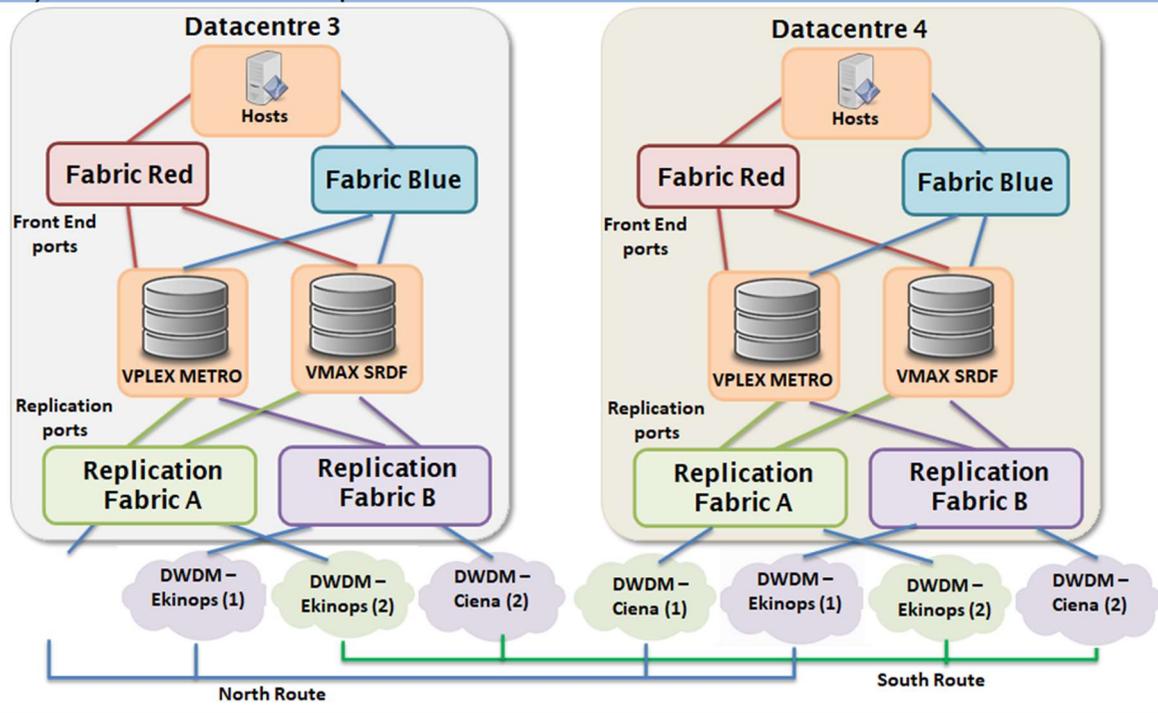
40GB Inter-Data Center link, two diverse routes.

Ethernet VPN delivers, two availability zone

Out of Band Management Access

VLANS Logically separate functions & clients

The Storage infrastructure is dual fabric leveraging the inter-site connectivity for replication using separate enterprise class storage for production and backup workloads.



Our solution adheres to a fault-tolerant architecture by leveraging the underlying resilience and high-availability of the hosting platform. All components will be deployable in a highly available mode, the application components are described in the following sections.

The database will be deployed across the two sites on dedicated compute using Oracle Real Application Clustering to deliver high-availability, leveraging the inter-site link for replication. In the event of a failure of the Active Database Node, the Passive Node will take over the workload.

The application components will be provisioned as multiple virtual machines working in tandem to deliver the solution workload requirements. VMware High Availability and VPLEX Replicated Storage delivers high-availability and disaster recovery across the two availability zones. In the event of a host failure within a site, Virtual Machines are moved to a standby available host. In the event of a Storage failure, replicated volumes become active in the alternate zone. In the event of a complete zone failure, virtual machines are restarted in the alternate zone.

Where required, load balancing will be used to balance workload across multiple web servers. In the event of a web server failure request are directed to the remaining health nodes.

The Site Reliability Engineering (SRE) approach ensures a continuous focus on identifying risk of non-availability and of addressing proactively.

This combination of SRE with network, storage, compute and application architecture delivers a fault-tolerant, highly-available architecture achieving and exceeding 99.9% availability.



Operational stability
and security

485 words

4.3e)

Recovery Strategy (RPO)

Weighting 0.80%
Technical Merit

Guidance:

In the event of an unforeseen failure with your primary hosting platform the solution must have a recovery strategy. This may be using the availability features of a public cloud provider or use of an alternative data centre in a private cloud deployment.

In all cases the solution must support a Recovery Point Objective (RPO) of the last committed transaction. The solution components need to support zero data loss when deployed in accordance with the Potential Provider's recommended architecture.

The recovery process must ensure that the security and integrity of the data is maintained throughout the process.

This requirement is not 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, in your response describe how your solution should be configured and/or operated in order to meet this overall requirement.

Your response should also identify any licensing implications for your overall solution.

We confirm that our solution fully meets the requirements for Recovery Strategy as detailed in requirements specification and that the solution architecture supports and RPO of zero through its architecture and capabilities.

As this requirement is already available for the current service, it will be included for Viable Product Release and the Operational Service Commencement Date. The architecture of the platform and the features described below enable delivery of an RPO of zero with zero data loss. The PIP solution has been architected to take advantage of these features.

Solution Recovery Strategy

Our solution, hosted on the IRIS UK Cloud Platform, our UK Government Secure multi-tenanted Cloud platform, delivers two availability zones connected via DWDM Bonded Fibre dedicated to Atos, thus maintaining data security, within synchronous replication distance. Along with the accompanying DELLEMC VPLEX Metro Storage and VMware vSphere High Availability enables a highly available cloud platform capable of delivering zero RPO for applications and services

Broadly there are two architectural models to deliver of zero RPO.

1. Applications are deployed at both sites and placed behind a load balancer; or in an active/passive state and utilise application/database replication. In the event of a site failure the alternate site takes the load for those service behind a load balancer; or for those application/database replicated services the cluster control plane will initiate a failover. An example of this is Oracles' Real Application Cluster (RAC) or Microsoft SQL Always On Availability
2. Applications are deployed to a single site and placed on replicated storage. In the event of site failure the virtual machines are restarted at the alternate site. This service is known as 'VMAutoRecovery' with encryption, thus maintaining data security.

Licensing of the infrastructure components that enable the features outlined in this section are included in the pricing provided e.g. DELLEMC VPLEX Metro Storage licensing.

Components of the PIP application utilise both features of the high availability capabilities of the platform outlined above. In the event of a site failure services protected by 'VM Auto Recovery', with encryption, will be restarted at the surviving site. This applies to application servers and web servers. Web servers are also further protected by load balancing. The load balancer is equally highly available across both availability zones.

Recovery Point Objective

The solution delivers an Oracle Real Application Clustering Database across the two availability zones of the platform. The Oracle RAC Database utilises VPLEX Metro (Replicated) Storage Volumes. In the event of a node failure, or site failure at the primary site the secondary site will take over service with zero data loss.

Network failover in the event site failure is controlled by dynamic routing protocols and the high availability features of VMware NSX.

Failover of Compute, Storage and Network components are automated, no manual intervention is required. Whole platform failover and tenant failover has been fully tested.



Operational stability
and security

The Buyer can be assured that with one of the key themes of our solution being operational stability and security , the Recovery Strategy is included by design.

500 words

4.3f) Recovery Strategy (RTO)	Weighting 0.80% Technical Merit
Guidance:	
<p>In the event of an unforeseen failure with our primary hosting platform the solution must have a recovery strategy. This may be using the availability features of a public cloud provider or use of an alternative data centre in a private cloud deployment. In all cases the solution must provide a Recovery Time Objective (RTO) of 3 hours.</p> <p>The solution components need to support timely service recovery when deployed in accordance with the Potential Provider's recommended architecture.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should include all High Level solution documentation required to meet the requirement.</p>	
<p>Introduction</p> <p>We confirm that our solution fully meets the requirement for Recovery Strategy and that the solution architecture support an RTO of three hours due to the architecture of the solution and the capabilities afforded to us by the Atos IRIS UK Cloud Platform.</p> <p>As this requirement is already available for the current service, it will be included for Viable Product Release and the Operational Service Commencement Date.</p> <p>Solution Recovery Strategy</p> <p>The IRIS UK Cloud Platform, our UK Government Secure multi-tenanted Cloud, delivers a platform of two availability zones connected via DWDM Bonded Fibre dedicated to Atos within synchronous replication distance. This, along with the accompanying DELLEMC VPLEX Metro Storage and VMware vSphere and NSX enables a highly available cloud platform capable of delivering low RTO for applications and services hosted on the platform.</p>	

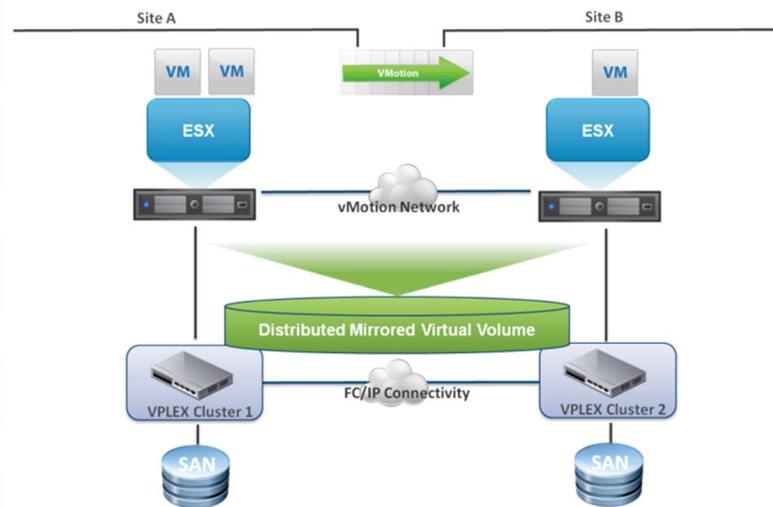
The IRIS UK Platform is hosted in two data centres within synchronous replication distance.

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.



There are multiple technologies to enable the delivery of the RTO.

1. Applications are deployed at both sites and placed behind a load balancer; in an active/passive state and utilise application/database replication. In the event of a site failure the alternate site takes the load for those services behind a load balancer; or for those application/database replicated services the cluster control plane will initiate a failover
2. Applications are deployed to a single site and placed on replicated storage. In the event of site failure, the virtual machines are restarted at the alternate site. This service is known as 'VMAutoRecovery'
3. Standard backup polices are available from Data Protection Level 1 through to Data Protection Level 8 these include application aware backups such as Oracle and SQ. See table below. For those DP levels which include replication restores can take place at the alternate site should the 'live' instance be corrupt and points 1 and 2 above of the platform architecture not be an option
4. Network ingress and egress is at the Primary Site. Dynamic routing allows the automatic failover of network ingress/egress should a network outage occur on the ingress/egress of the primary site.

Data Protection Description	Service Level Option							
	1	2	3	4	5	6	7	8
1 full backup per week	X	X	X	X	X	X	X	X
6 incremental backups per week		X	X	X	X	X	X	X
Backups retained for 28 days	X	X	X	X	X	X	X	
Backups retained for 90 days								X
1 full backup per month retained for 12 months			X		X	X	X	X
1 full backup per year retained for 7 years			X		X			X
Backups retained on local site	X	X	X			X		
Backups retained offsite				X	X		X	X

Multiple tenants have taken advantage of these features to build highly available applications and databases e.g. a financial services customers core banking engine and a utility suppliers payment gateway.

Recovery Time Objective

The proposed solution leverages all of the platform capabilities outlined above to deliver an RTO of 3 hours. To summarise:

1. High Availability NSX Edge Service Gateways (Load Balancer and Firewalls)
2. Internet, WAN and Paragon Connectivity out of the Primary and Secondary Sites
3. Load Balanced PRS Application and ForcePoint Proxy across the two availability zones
4. Leveraging Replicated Storage for VM Auto Recovery for PRS, Siebel, Data Stage and other supporting services
5. SQL Server Always On Availability Cluster – Active / Passive across the two availability zones
6. Oracle Real Application Cluster – Active / Passive across the two availability zones
7. Replicated NAS Storage for PRS, GlobalScape, User Profiles, Back Office Apps.



Operational stability
and security

476 words

4.3g) Security Verification Standards	Weighting 0.50% Technical Merit
Guidance:	
<p>Your solution should be designed to be verified against any application security verification standards (e.g. OWASP ASVS). https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, in your response describe where any such security verification standards can be applied and can be verified.</p>	
<p>Introduction</p> <p>Our solution fully meets the requirements for Security Verification Standards. The foundations to our solution are inherited from our current services supporting PIP, whilst refining and enhancing those capabilities, and this approach enables us to meet the Operational Service Commencement Date.</p> <p>Atos maintains strong links with industry vendors, ensuring that we remain at the leading edge of application security research. By leveraging this expertise and adopting ‘Secure by Design’ principles throughout the Software Development Lifecycle (SDLC), we develop applications that securely protect classified information and data.</p> <p>Securing the Applications</p> <p>Our solution ensures end-to-end security with "defence-in-depth" for administrative, technical, and physical controls and employs secure coding practices, "security by design" principles and industry-leading application security testing throughout the SDLC.</p> <p>Our security verification process will:</p> <ul style="list-style-type: none"> • Ensure logging is functioning • Check events are classified consistently, and the field names, types and lengths are correctly defined • Ensure no unwanted side-effects from logging • Check the effect of loss of external network connectivity on logging mechanisms • Ensure logging cannot be used to deplete system resources and lead to denial of service • Test the effect of logging failures • Verify access controls on the event log data. <p>For the Application Penetration Testing, we will:</p> <ul style="list-style-type: none"> • Ensure logging is implemented and enabled during application security, penetration and performance testing • Test the mechanisms are not susceptible to injection attacks. 	

Verification and Evidence of Application Security

Code commits will be signed and verified in GitHub enabling an administrator or auditor to track events to a specific developer.

Releases are comprised of multiple code commits. Full chain-of-custody reporting for released code will be available using GitHub.

GitHub will be configured to enforce signed code, and cannot be bypassed by developers.

Enforcing Application Pipeline Security

The CI/CD pipelines will include inbuilt security controls and can only be modified by Privileged Access User, which will be fully tracked and auditable.

Code commits that fail the CI/CD pipeline tests including SCA, SAST and DAST will be prevented from being merged into the release. Remediation recommendations will be fed back to the developer using GitHub, SonarQube, OWASP ZAP and Snyk.

Managing open-source vulnerabilities

Open-source code libraries and components will be scanned utilising various toolsets.

Our solution has the advantage of utilising RASP machine learning from Palo Alto Prisma. Additional tools, including Harbor, OWASP ZAP and OpenSCAP will provide the necessary tooling to ensure container security.

Any new vulnerabilities discovered will be imported into the scanning tooling for checking. With these updates, Prisma, Snyk, SonarQube, Harbor and OpenSCAP will be able to identify these new vulnerabilities in running applications

Managing Security of re-used Microservices

Digital signing of code at commits and deployment will be fully tracked and auditable using GitHub. The proven Palo Alto Prisma tool will proactively mitigate any issues of flawed code, which has been heavily re-used, by actively looking for anomalous behaviours and, depending on a pre-defined policy, can take automated response actions to prevent damage.



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

500 words

4.3h)

Vulnerability Management

**Weighting 0.50%
Technical Merit**

Guidance:

Your solution should be supported by tooling and processes to ensure technical vulnerability is detected and remedied and in a timely manner. The provision will likely include:

- Core components hardened in accordance with a recognised hardening standard e.g. Centre for Internet Security (CIS)
- Software development is undertaken in accordance with secure coding standards, and any code which could result in vulnerability is detected and remedied prior to release. Static Code Analysis could be employed for example.
- Applicable security patches are identified, tested, and deployed in a timely manner.
- Vulnerability scanning runs regularly and any vulnerability discovered is remedied in a timely manner.
- The solution is subject to penetration testing prior to go-live, and no less frequently than annually, or following significant change, going forward.

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, in your response provide brief details of your vulnerability management capability.

Introduction

Our solution fully meets the requirements for Vulnerability Management. The foundations to our solution are inherited from our current services supporting PIP, whilst refining and enhancing those capabilities enabling us to meet the Operational Service Commencement Date.

The solution is hosted on our secure IRIS Platform. IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads.

This platform and our overall solution is supported by tooling and processes to ensure that technical vulnerabilities are detected in a timely manner.

Vulnerability Management Capability

The Client Security Manager is responsible for managing and tracking vulnerabilities for all components of the service.

A vulnerability scanning tool will be used as part of Vulnerability Management to regularly scan the customer infrastructure for service and host vulnerabilities, on a scheduled basis.

A monthly vulnerability compliance report is presented to the IRIS Security Working Group (SWG) to which the Buyer's security representatives are invited. An ad hoc SWG will be called if required to approve actions to address any identified critical vulnerabilities.

Component Hardening

The IRIS Platform offers 'component hardening including other platform components including Networking, Storage and Compute equipment in line with either CIS Benchmarks or vendor recommendations. The IRIS platform is 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.

Compliance metrics will be produced to evidence how the solution meets relevant guidance and "Security-by-Design" principles.

Security Patches

Security Patches are identified, tested and 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.

Vulnerability Scanning

Atos will provide a vulnerability scanning tool 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.

Scan engines execute monthly vulnerability scans and forward results to the Management Server. Queries and reports are created via the user interface where administrators define and schedule the vulnerability scans.

Penetration Testing

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



Operational stability
and security

482 words

4.3i)

Scaling Capability – UI Interaction

**Weighting 0.30%
Technical Merit**

Guidance:

The Buyer has a requirement for the solution to provide a maximum response time of 2.5 seconds for all agent user interface interaction, for 99.00% of the time during business hours. The timing is measured at the solution’s boundary (i.e. client facing external interface) to the agent user interface (i.e. user’s).

This requirement is not required for Viable Product Release (See Attachment 6.1)

This requirement is required for Operational Service Commencement Date (See Attachment 6.1)

Question:

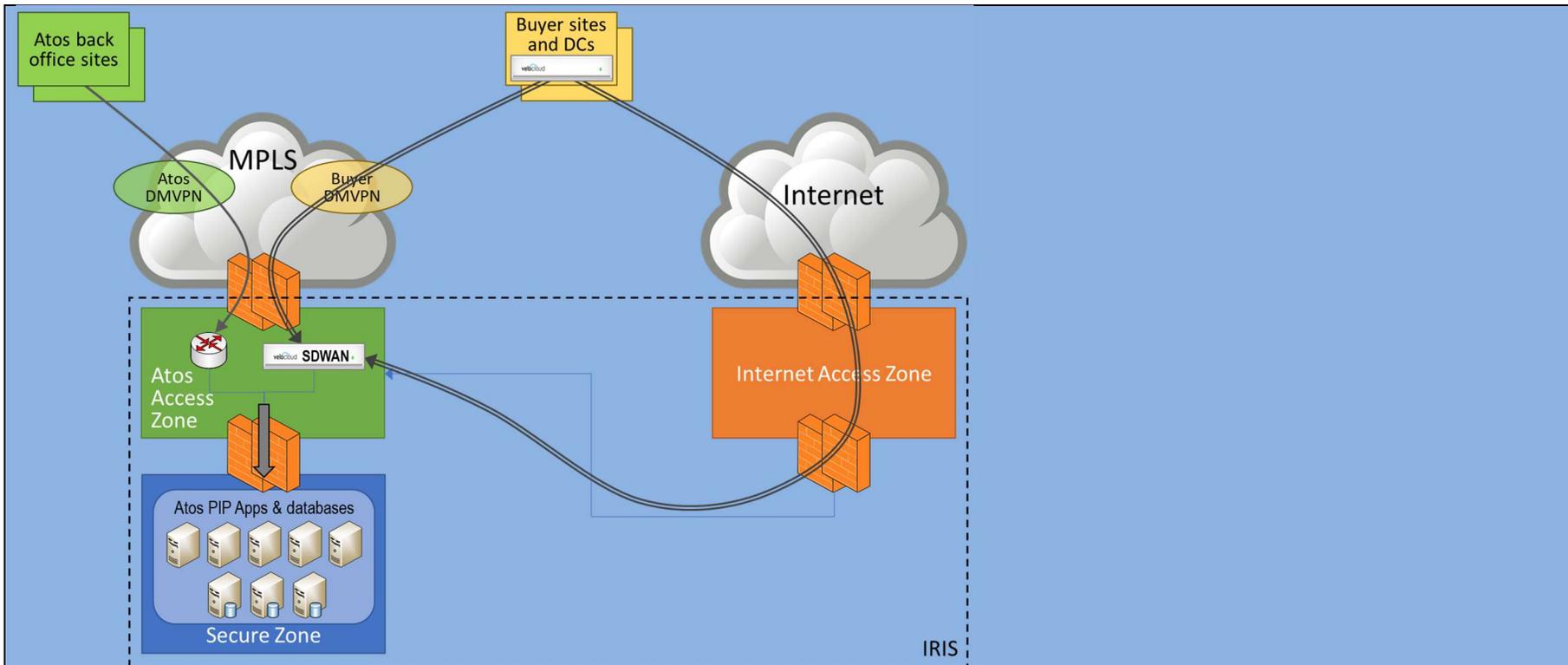
Incorporating the guidance above, in your response describe your solution’s scaling capabilities for responding to fluctuating demands placed on the solution’s components by user interaction. Clearly state where scaling impacts licensing/commercial aspects of your solution.

We confirm that our solution fully meets the requirement for Scaling Capabilities for responding to fluctuating demands placed on the solution’s components by UI interaction and that as this requirement is already available, it will be included within the for Viable Product Release and by the Operational Service Commencement Date.

Connectivity between the proposed solution’s external interface and the Buyer is via a dedicated WAN link to facilitate access to the Buyer’s hosted PIP applications via Atos’s centrally managed Citrix desktop solution.

The assumption is that the Buyer will continue to use this existing link based on a BT IP Connect MPLS service. The CDR will be flexed up or down depending on the live load. DMVPN encryption will be used to protect data in transit to RESTRICTED IL3.

Functional probes will be used to monitor representative application journeys and report back typical user experience times and where thresholds are breached.



There is also the opportunity to extend the Buyer's SDWAN across both the MPLS and Internet connections into the IRIS** Atos Access Zone, thereby further optimising the user experience by allowing network traffic to take the most efficient path to the Atos PIP solution.

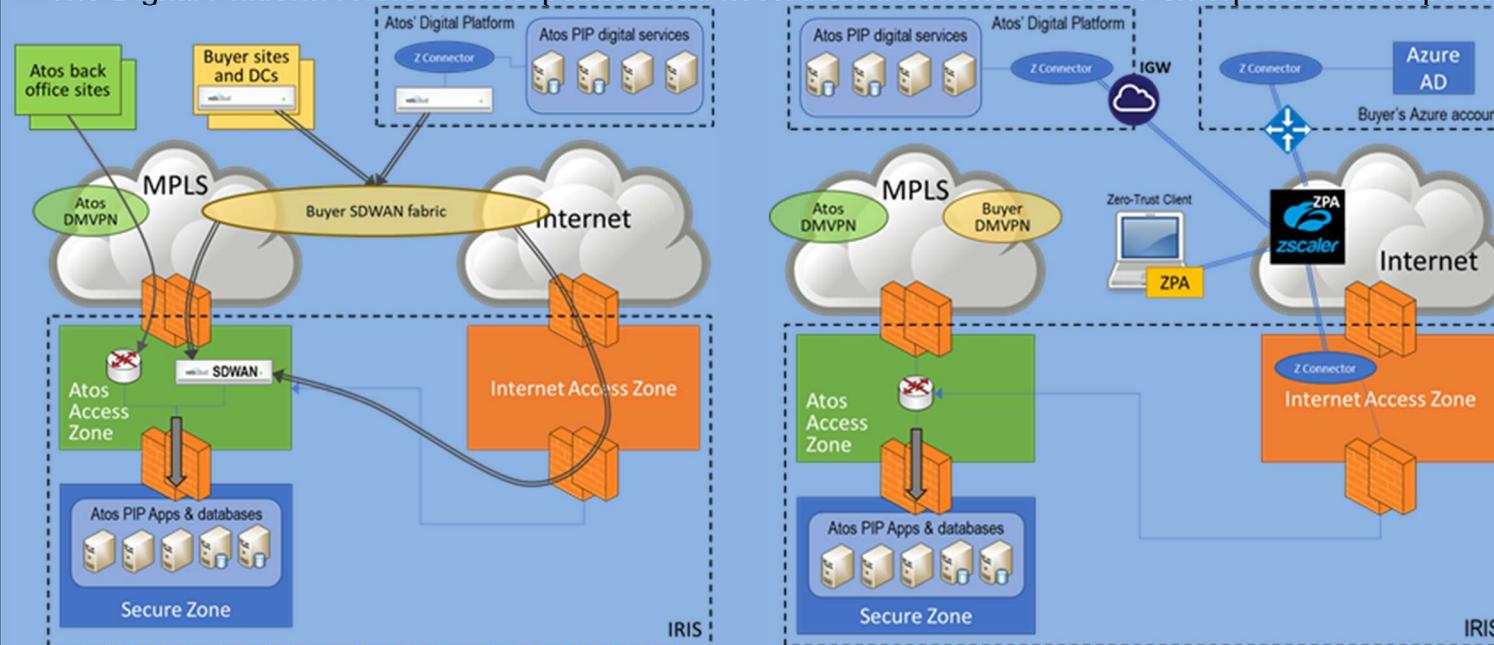
** IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads.

The combination of real-time SDWAN proactive link remediation and monitoring as well as representative user experience probes provide a holistic view of the solutions behaviour and the ability to proactively respond to potential capacity issues. If the user interaction SLA of <2.5sec, 99% of the time is being threaten and/or approaching capacity issues are identified an investigation can proactively be made into the networking infrastructure interlinking the client and the Buyer. This may, for example, result in:

- Increasing the priority of the application traffic across the SDWAN
- Increasing the private and/or public WAN links to reduce latency.

With a possible move to Atos' Digital Platform⁺⁺ for new or upgraded functional modules/components if appropriate, access to cloud hosted resources can also be enhanced by SDWAN to provide forward error correction and TCP optimisation or by zero-trust network solutions such as Zscaler. Either solution would need agreement to be made between both parties.

⁺⁺ The Digital Platform refers to Atos' public cloud hosted environment for secure enterprise consumption of AWS services.



SDWAN

Zscaler



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

410 words

4.3j) Scaling Capability – APIs	Weighting 0.30% Technical Merit
Guidance:	
<p>The Buyer has a requirement for the solution APIs to provide a maximum response time of < 50ms, 99.00% of the time. The timing is measured at the solution’s API service end-point prior to network egress.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, in your response describe your solution’s scaling capabilities for responding to fluctuating demands placed on the solution’s components by API calls. Clearly state where scaling impacts licensing/commercial aspects of your solution.</p>	
<p>We confirm that our solution fully meets the requirement for Scaling Capabilities for responding to fluctuating demands placed on the solution’s API components by user interaction, and that as this requirement is already available, it will be included within the Viable Product Release and by the Operational Service Commencement Date.</p> <p>All applications and databases for the proposed solution are hosted within the IRIS UK Cloud Platform on virtual server infrastructure. IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads.</p> <p>Virtual machines are monitored in terms of CPU, memory and disk with appropriate threshold alarms to alert against approaching capacity issues.</p> <p>In addition, API probes monitor representative application interactions and report back response times and where thresholds are breached.</p> <p>The combination of infrastructure and representative user experience monitoring provides a holistic view of the APIs behaviour and the ability to proactively respond to potential capacity issues.</p> <p>If the API SLA of <0.5ms, 99% of the time is being threatened and/or approaching capacity issues are identified an investigation can proactively be made into the application, infrastructure and networking components used to support the service. This may, for example, result in:</p> <ul style="list-style-type: none"> • The number of programmatic API instances being increased • Scaling the virtualised infrastructure either vertically or horizontally • A combination of measures. <p>without the need for re-platforming or impacting the functional behaviour of the applications they host.</p> <p>In line with our drive to digitalise customer systems and service operations, moving to Atos’ Digital Platform for new or upgraded functionality will be assessed and if appropriate developed on this platform.</p>	

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, native applications.

This will allow additional exploitation of microservices architecture and scaling capacity can be further enhanced by using:

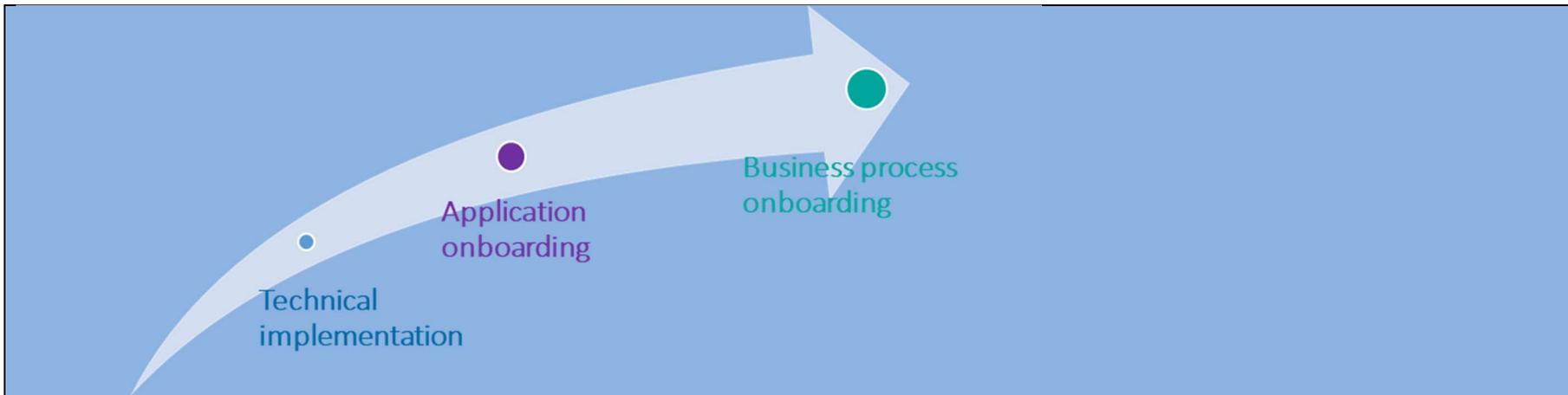
- containerisation for APIs/services
- highly scalable and performant container management services as well as
- automatic scaling of containers and underlying cloud compute resources; capacity can dynamically be adjusted to maintain steady and predictable performance at the lowest possible cost. This is not only used for increasing capacity of constrained resources when demand increases but also removes excess capacity when demand drops.

Where possible serverless architectures will be employed to avoid having to manage or even configure automatic capacity scaling.



410 words

4.3k) Response Time Measurement	Weighting 0.30% Technical Merit
Guidance:	
<p>The solution must be configurable to enable response time measurements to be captured, as required, to support the analysis of performance problems. The design must allow data collected to be of sufficient granularity to meet the needs of performance investigation. This includes the ability to report on the segmentation of elapsed times across solution components.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, in your response describe your solution’s capabilities for supporting response time measurements.</p>	
<p>We confirm that our solution fully meets the requirement for Response Time Measurements (RTMs), and that as this requirement is already available, it will be included within the Viable Product Release and by the Operational Service Commencement Date.</p> <p>Real Time Application Measurement will be supported by our Digital Performance Management (DPM) system which drives efficiency by maximising the performance of business-critical applications supporting our solution.</p> <p>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.</p> <p>Atos offers a modular implementation & service approach to suit the needs of the solution. The DPM service offers three levels of implementation:</p> <ul style="list-style-type: none"> • Technical implementing the DPM OneAgent(s) onto the servers which host the solution as well as ActiveGates for synthetic monitoring of internal web interfaces and API end-points where in scope. This is undertaken through an onboarding process working with key stakeholders, identifying servers hosting critical business applications and technically installing agents on the servers • Onboarding of applications to improve the Dynatrace configuration of the applications and corresponding services, processes and hosts. This phase focuses on improving the Dynatrace OneAgents configurations implemented in the technical Implementation • Onboarding of business processes and the corresponding KPI’s. This level of service is focused on business processes enabling us to perform process management based on Dynatrace. The object is to monitor each step of the business process and report on the defined KPI’s. Dynatrace dashboard containing an overview of the business process steps and KPI’s is developed. 	



Monitoring is executed from 2 separate AWS locations at an agreed frequency, measuring the availability, key server metrics (CPU, Memory, Disk) and the elapsed time to complete user journeys and execute application end-points.

The DPM platform needs 7 days to baseline normal behaviour. Dashboards will have data shortly after the activation of agents. Monitoring and standard reporting provide a clear overview of positive and negative trends in elapsed times allowing us to understand live and anticipated performance of services, identifying possible issues leading to resolution activities before they impact the solution.

Granularity and segmentation can be further tailored to meet the customer's and the solution's needs based on DPM's modular approach. However, this will come with additional commercial and licensing impacts. This is undertaken through an application onboarding process which looks to tailor and improve the configuration of OneAgents implemented in technical onboarding. For example, charting key user actions and service steps.

This could be done at a high-level splitting network versus server processing versus client-side rendering times in an application page load or could be further broken down to, for example, time spent on DNS resolution, TCP/SSL socket establishment, request redirects etc.

The DPM platform supports collection and monitoring of performance metrics and trends on multiple levels. Technical implementation of DPM agents will meet the ability to capture RTMs and support the analysis of performance related problems and can be further enhanced.

495 words



Improve user and
citizen experience

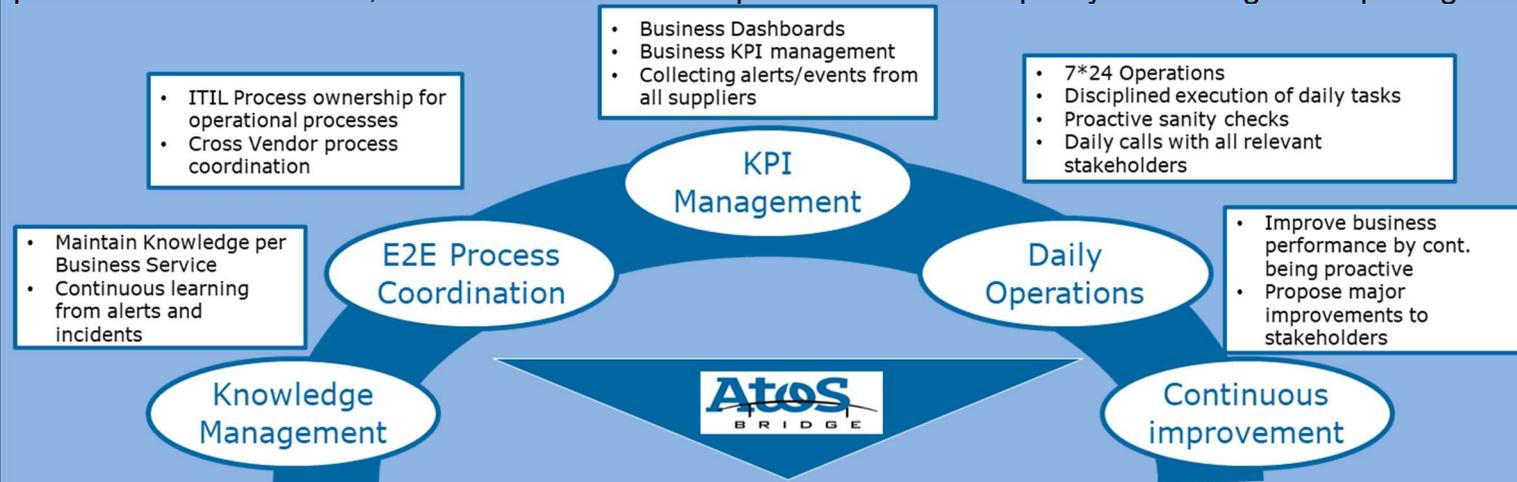


Operational stability
and security

4.3I) Application Management	Weighting 0.30% Technical Merit
Guidance:	
<p>All proposed solution components must provide a capability to log/report on status showing details of warnings, errors, unavailability or degraded states as appropriate.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, in your response describe your solution's monitoring and control capabilities. In your description detail any monitorable services, queryable health endpoints, log formats, user interface monitoring frameworks, etc.</p>	
<p>Introduction</p> <p>We confirm that our solution fully meets the requirement for Application Monitoring, and that as this requirement is already available, it will be included within the for Viable Product Release and by the Operational Service Commencement Date.</p> <p>Event Monitoring and Analysis Framework</p> <p>Atos will implement its state-of-the-art monitoring service, called AtosBridge, to monitor all components and services that form part of our solution.</p> <p>AtosBridge uses a combination of Servicetrace, Elastic and Beats to monitor application performance on an availability and functional level.</p> <p>AtosBridge tooling, integrated with Atos' ServiceNow platform, will monitor the components and services, and provide event and warning data in real-time, within ServiceNow.</p> <p>Based on historical and functional data, Atos creates an image of normal application behaviour. Using this data, our monitoring toolkit detects anomalies: i.e., any application behaviour that is not expected. Examples are:</p> <ul style="list-style-type: none"> • Degraded application performance, including slow response times • Unanticipated database growth. <p>Utilising ServiceNow's Event Management module and pre-defined rulesets, an event will automatically be raised when certain thresholds have been breached. This will be routed to the responsible application team, enabling pro-active investigation and preventing user impact.</p> <p>Proactive Event Resolution</p> <p>Events or incidents raised within AtosBridge and ServiceNow will be resolved automatically, wherever possible, using our cutting-edge automation tools. SyntBots, Task Bots and the ServiceNow Orchestration module will be used to automatically perform runbook-based operations on the service to resolve events and incidents.</p>	

One of the tools powering AtosBridge is Elastic. Elastic collects all logs and event data, making this data available through Atos Bridge dashboards (which are, in turn, available via ServiceNow). This will make huge amounts of data searchable in meaningful ways. Threshold-based checks can be extended or replaced by real-time anomaly detection (powered by the Elastic search Machine Learning engine). This will support analysing the data to understand the live and anticipated performance of the services, identifying possible issues and triggering resolution activities before they impacted the service.

Application Monitoring
 The AtosBridge monitoring capability is well suited for application monitoring as it provides a coherent end-to-end view, including application events, management dashboards, diagrammatic representations of operational status, real-time performance dashboards, historical trend data and performance and capacity monitoring and reporting.



End 2 End Business Process Chain Management

The AtosBridge monitoring solution will ensure all application touchpoints are adequately monitored, and corrective action is taken ahead of time to prevent any major incident from occurring. This includes warnings, errors, unavailability or degraded states as required.

AtosBridge will combine information collected from various sources to ensure a controlled, stable, and coordinated day-to-day running of the proposed PIP applications and services. Sources include log files in multiple formats (including common/extended), availability endpoints, network traffic data, digital cloud data/events and metrics for numerous services. AtosBridge uses Beats to capture standard metrics, but can also support extending or creating entirely new Beats modules to capture any type of data. This proactive monitoring will ensure that the interfaces continue to be available to the applications and wherever possible disruption is avoided or minimised.



Operational stability
and security

490 words

4.3m)	Buyer Security Standards		Weighting 0.40% Technical Merit						
Guidance:									
<p>The link below navigates to the Buyer procurement: Security Standards and policies. https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards 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)</p>									
Question:									
<p>Incorporating the guidance above, in your response describe:</p> <ul style="list-style-type: none"> • Which standards are relevant to your proposed solution? • Which of the relevant standards is your proposed solution compliant with? • Which of the relevant standards is your proposed solution not compliant with? Please explain why, and (if applicable) how you will become compliant within your current product roadmap 									
<p>Introduction Our solution is compliant with the Buyer’s security policies and standards. Our solution utilises currently provided capabilities as a foundation, to be refined and enhanced as appropriate in meeting additional requirements. This minimises development and underpins our assurance of making the required capabilities available for the Viable Product Release and the Operational Service Commencement Date. Buyer Security Standard Compliance Our solution will be hosted on the IRIS UK Cloud Platform. <i>IRIS is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based Security Cleared resources, designed for Official/Official Sensitive workloads for which a comprehensive suite of Atos security-related policies and standards already exist.</i> The suite of IRIS UK security policies are aligned with, the requirements of the Buyer’s security policies and standards. The IRIS UK Platform operates its own Security Working Group (SWG) chaired by a UK based Operational Security Manager. At each meeting, an operational security report is presented covering security-related topics including security compliance, patching and antivirus status, security incidents, security deltas, security exceptions, security vulnerabilities and threat updates. The SWG will provide ongoing monitoring of our compliance with applicable security policies and standards. The following table identifies policies that are relevant to our solution, and those we comply with.</p> <table border="1" data-bbox="416 1343 1850 1453"> <thead> <tr> <th data-bbox="416 1343 1211 1453">(108) Policy</th> <th data-bbox="1211 1343 1529 1453">(109) Relevant to our solution?</th> <th data-bbox="1529 1343 1850 1453">(110) Is our solution Compliant?</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				(108) Policy	(109) Relevant to our solution?	(110) Is our solution Compliant?			
(108) Policy	(109) Relevant to our solution?	(110) Is our solution Compliant?							

(111) Acceptable Use Policy	(112) Yes	(113) Yes
(114) Information Management Policy	(115) Yes	(116) Yes
(117) Personnel Security Policy	(118) Yes	(119) Yes
(120) Physical Security Policy	(121) Yes	(122) Yes
(123) Cryptographic Key Management Policy	(124) Yes	(125) Yes
(126) Email Policy	(127) Yes	(128) Yes
(129) Forensic Readiness Policy	(130) Yes	(131) Yes
(132) Microsoft Teams Recording and Transcription Policy	(133) Yes	(134) Yes
(135) Privileged Users Security Policy	(136) Yes	(137) Yes
(138) Remote working security Policy	(139) Yes	(140) Yes
(141) Security Classification Policy	(142) Yes	(143) Yes
(144) SMS Text Policy	(145) Yes	(146) Yes
(147) Social Media Policy	(148) No	(149) Yes
(150) Technical Vulnerability Management Policy	(151) Yes	(152) Yes
(153) User Access Control Policy	(154) Yes	(155) Yes
(156) Common Standards for Identity Verification and Authentication (CSIVA) of DWP customers	(157) Yes	(158) Yes
Schedule 29 Access and Authentication Controls SS-001 (part 1)	(159) Yes	(160) Yes
Schedule 30 Privileged User Access Controls SS-001 (part 2)	(161) Yes	(162) Yes
Schedule 31 Public Key Infrastructure & Key Management (SS-002)	(163) Yes	(164) Yes
Schedule 32 Software Development (SS-003)	(165) Yes	(166) Yes
Schedule 33 Database Management System Security Standard (SS-005)	(167) Yes	(168) Yes
Schedule 34 Security Boundaries (SS-006)	(169) Yes	(170) Yes

Schedule 35 Use of Cryptography (SS-007)	(171) Yes	(172) Yes
Schedule 36 Server Operating System (SS-008)	(173) Yes	(174) Yes
Schedule 37 Hypervisor (SS-009)	(175) Yes	(176) Yes
Schedule 38 Desktop Operating System (SS-010)	(177) Yes	(178) Yes
Schedule 39 Containerisation (SS-011)	(179) Yes	(180) Yes
Schedule 40 Protective Monitoring Standard - For External Use (SS-012)	(181) Yes	(182) Yes
Schedule 41 Firewall Security (SS-013)	(183) Yes	(184) Yes
Schedule 42 Security Incident Management (SS-014)	(185) Yes	(186) Yes
Schedule 43 Malware Protection (SS-015)	(187) Yes	(188) Yes
Schedule 44 Remote Access (SS-016)	(189) Yes	(190) Yes
Schedule 45 Mobile Device (SS-017)	(191) No	(192) Yes
Schedule 46 Network Security Design (SS-018)	(193) Yes	(194) Yes
Schedule 47 Wireless Network (SS-019)	(195) No	(196) Yes
Schedule 48 Voice & Video Communications (SS-022)	(197) No	(198) Yes
Schedule 49 Cloud Computing (SS-023)	(199) Yes	(200) Yes
Schedule 50 Virtualisation (SS-025)	(201) Yes	(202) Yes

Schedule 51 Application Security Testing (SS-027)	(203) Yes	(204) Yes
Schedule 52 Microservices Architecture (SS-028)	(205) Yes	(206) Yes
Schedule 53 Securely Serving Web Content (SS-029)	(207) Yes	(208) Yes
Schedule 54 Oracle Database Security (SS-030)	(209) Yes	(210) Yes
Schedule 55 Domain Management (SS-031)	(211) No	(212) Yes
Schedule 56 Security Patching (SS-033)	(213) Yes	(214) Yes

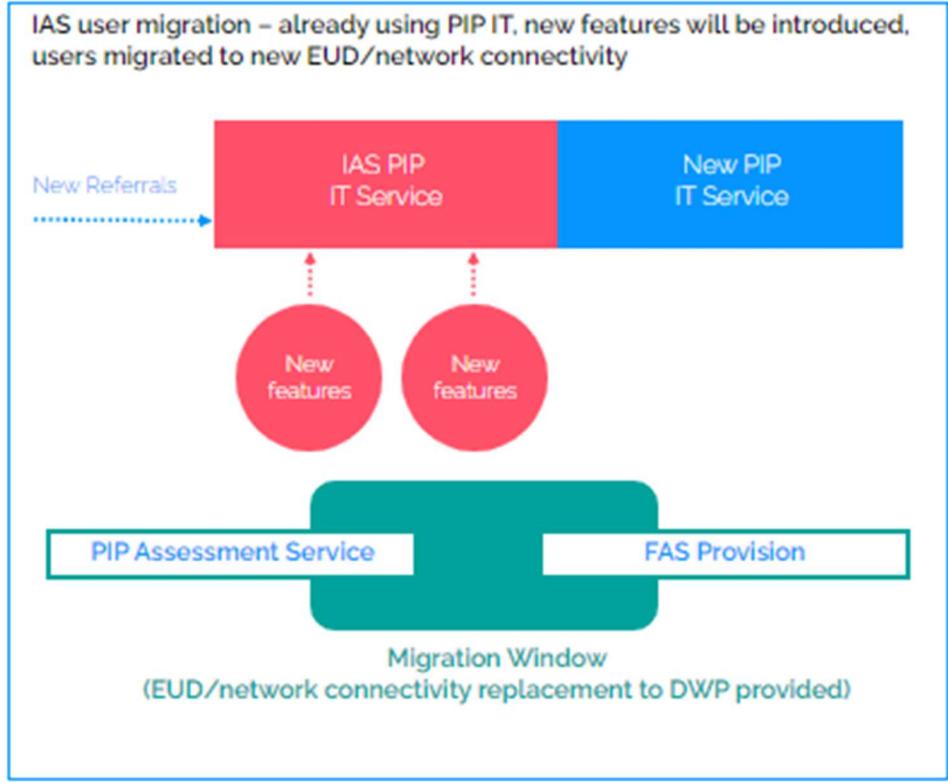


Operational stability and security

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

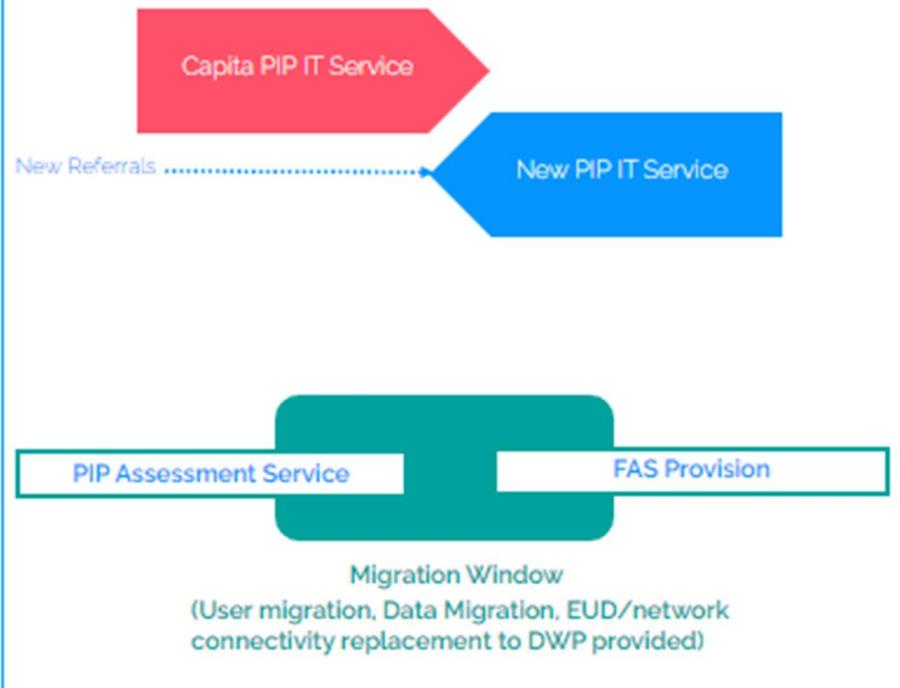
496 words

4.3n)	Migration	Weighting 1.00% Technical Merit
Guidance:		
<p>The solution response should include details of migration of personal, operational and any pertinent reference data to the new solution. This migration of data should be in line with, and support, the overall transition approach.</p> <p>Data will include, but not be limited to, the following:</p> <ul style="list-style-type: none"> • Residual Inflight referrals and their associated assessment data including contact history and further medical evidence requested. • Full citizen contact history • Historic referral and assessment data • Inflight and historic assessment Audit data • Expense claims, current and historic • Complaint data, current and historic • Health care professional data • Assessment locations data, including current room bookings and room availability. • Historic MI data <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, in your response explain how your solution would facilitate this migration from the incumbent IT systems as part of the transition.</p>		
<p>Compliance Our solution fully meets the requirement for Migration and this will be included for Viable Product Release and by the Operational Service Commencement Date.</p> <p>Scope As our solution is founded on the IAS services in operation today, this negates the requirement to migrate any of the data from current Lots 1 and 3 (Lots 1, 3, 4 of the new procurement).</p> <p>The migration of data will focus on Capita data for Lots 2 and 4, currently held in their Core Referral and Scheduling Data System and their MI data</p> <p>Data Migration Our migration activities are shown in the following diagrams. The first demonstrates our approach for IAS users</p>		



For the Capita users, we will follow the 'ramp-up and drain down' migration approach to maintain continuity of service over the transition.

Capita user migration – Ramp up/Drain Down



This will facilitate Capita to 'drain down' over a twelve week period post the initial transition start date to continue processing existing in-flight cases within their system until they are closed.

Whilst Capita conclude their in-flight cases, Atos will 'ramp-up' by entering and processing new cases from the other current Lots using their Practitioner Referral System (PRS) and Siebel Appointment Manager (SAMS).

It is assumed that we will not migrate in-flight applications. To avoid in-flight referrals in the migration process, the planned solution is to migrate all Capita data at the end of the transition period when the cases are closed. Prior to the full migration there will be development testing of the migration process using subsets of the data to ensure the integrity of the process.

The migration will ingest data using the Datastage ETL tool from an export provided by Capita creating a skeleton claimant record in the PRS system containing claimant specific data including NINO, Name, DoB, Contact Details and gender.

There will be no migration of in-flight referrals. Contact history, historic data, audit data, expense claims, complaint data and any other data identified as required will all be migrated and sit on the Atos databases. This data will be accessible to view from the skeleton claimant record.

The preferred practice for Health Care Professionals is that those not on the current PRS system will not be migrated but treated as new joiners and manually entered. Similarly, assessment locations not on the Atos system will also be manually entered. Manually entering Health Care Professional and Assessment Location data will help reduce the time and effort spent on the migration solution development.

For MI Data the relevant fact and dimensions tables will be migrated allowing for queries and reports to be run against this data. The data will sit on Atos databases but will stay as an archive of Capita MI data and will not be joined to Atos MI data.

Atos have experience in data migration with recent clients including [Redacted FOIA S43 Commercial Interest] where many millions of records were migrated from nine source systems.



Quickest, safest
transition

The Buyer can be assured that one of the key themes of our solution is a quick and safe transition

497 words

4.3o)	Third Party Software	Weighting 0.20% Technical Merit
Guidance:		
<p>Please list all (mandatory and optional) third party software that will be used for the solution. These could be:</p> <ul style="list-style-type: none"> • Data integration software • Application integration (middleware) • Reporting • Visualisation • AI services • Development tools • Etc. <p>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)</p>		
Question:		
<p>Incorporating the guidance above, and consistent with Attachment 5 your response should detail all software required. Detailing how it will support the delivery of the Viable Product Release and the Operational Service Commencement, in line with the dates specified in Attachment 6.1.</p>		
<p>We confirm that our solution fully meets the Non-Functional Requirement for Third party software, and that as this requirement is already available, it will be included within the Viable Product Release and by the Operational Service Commencement Date. The following tables are in Attachment 5 - but are also included also below.</p> <ol style="list-style-type: none"> 1. Supplier Software <p>The Supplier Software includes the following items:</p>		

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Type (COTS or NonCOTS)	Term/expiry
JBoss	Red Hat	Application platform	per RHEL	None	COTS	Annual subscription
Red Hat Decision Manager Standard	Red Hat	Platform management	2	None	COTS	Annual subscription
Red Hat Decision Manager Premium	Red Hat	Platform management	1	None	COTS	Annual subscription
Siebel	Oracle	Database	Multiple (breakdown can be provided)	None	COTS	Annual subscription
Oracle	Oracle	Database	Multiple (breakdown can be provided)	None	COTS	Annual subscription
InfoSphere DataStage	IBM	DataStage Workgroup Edition Processor	140	None	COTS	Annual subscription
IBM Cognos Analytics Explorer Authorized	IBM	IBM Cognos Analytics Explorer Authorized User Annual SW Subscription & Support	7	None	COTS	Annual subscription
IBM Cognos Analytics Administrator	IBM	IBM Cognos Analytics Administrator per Authorized User Annual SW Subscription & Support	3	None	COTS	Annual subscription
IBM Cognos Analytics User	IBM	IBM Cognos Analytics User Authorized User Annual SW Subscription & Support	20	None	COTS	Annual subscription
IBM InfoSphere DataStage and QualityStage Designer	IBM	IBM InfoSphere DataStage and QualityStage Designer Concurrent User Annual SW Subscription & Support	5	none	COTS	Annual subscription

NEOTYS	ASM Technologies	Gold Support renewal for NeoLoad License	1	none	COTS	Annual subscription
Hopewiser ABV	ASM Technologies	Licence to use Address Server & Bankcoder PIP Production & Licence to use Address Server & Bankcoder PAF	1	none	COTS	Annual subscription
Oracle Database	Oracle	Oracle database licensing	2	none	COTS	Annual subscription
Atlassian	ASM Technologies	JIRA	25	none	COTS	Annual subscription
Flexera for clients	Flexera	Software licencing reporting	300	none	COTS	Perpetual license
Flexera for Data Centers	Flexera	Software licencing reporting	200	none	COTS	Perpetual license
VisualSVN	ASM Technologies	VisualSVN is an Apache Subversion client, implemented as a low-level VS package extension for Microsoft Visual Studio, that provides an interface to perform the most common revision control operations directly from inside the Visual Studio IDE.	1	none	COTS	Annual subscription
Symantec SSL	ASM Technologies	Certificate for DWP PIP Account for the AP Automation project	2	none	COTS	Annual subscription
Red Hat	Red Hat Enterprise Linux	Certified Cloud and Service Provider (CSSP) License and Maintenance	26	none	COTS	Annual subscription
Microsoft	Windows Server	Service Provider Licensing Agreement (SPLA) License and Maintenance	67	none	COTS	Annual subscription

Microsoft	Systems Center	Service Provider Licensing Agreement (SPLA) License and Maintenance		none	COTS	Annual subscription
Intel	McAfee	McAfee Virus Scan, McAfee End Point Security, McAfee ePolicy Orchestrator		none	COTS	Annual subscription
JBoss	Red Hat	Support Contract os only		none	COTS	Annual subscription
Symantec SSL	ASM Technologies	Certificate for DWP PIP Account for the AP Automation project		none	COTS	Annual subscription
Globalscape EFT	Globalscape	Secure file transfer		none	COTS	Annual subscription
Globalscape DMZ Gateway	Globalscape	DMZ gateway services		none	COTS	Annual subscription
Forcepoint Proxy	Forcepoint	Web Proxy for servers outbound		none	COTS	Annual subscription
Tripwire	Tripwire	VSS Vul scanning service device profilers		none	COTS	Annual subscription
Tripwire	Tripwire	VNE Manager		none	COTS	Annual subscription
Tripwire	Tripwire	TripWire Subscription licence 122 endpoints		none	COTS	Annual subscription
VMware	vSphere	vSphere		none	COTS	Annual subscription
VMware	NSX	NSX		none	COTS	Annual subscription
VMware	vRealize	vRealize Operations Manager, vRealize Orchestrator, vRealize Automation, vRealize Log Insight		none	COTS	Annual subscription

Juniper	QFX	Virtual Chassis Fabric Licensing (12 devices)		none	COTS	Annual subscription
Juniper	EX	EX Licensing (4 devices)		none	COTS	Annual subscription
Juniper	MX	MX Licensing (4 devices)		none	COTS	Annual subscription
Juniper	SRX	Secure Edge SRX Licensing		none	COTS	Annual subscription
Juniper	Space	JunOS Space Network Management Platform		none	COTS	Annual subscription
Juniper	Security Director	JunOS Space Security Director (5 devices)		none	COTS	Annual subscription
Juniper	Network Director	JunosOS Space Network Director (25 devices)		none	COTS	Annual subscription
Juniper	Maintenance	Annual Software\Hardware Maintenance		none	COTS	Annual subscription
Fortinet	Forti Manager	Forti Manager (1 Device), 25 vDOM's		none	COTS	Annual subscription
Fortinet	Forti Analyzer	Forti Analyzer (1 Device), 6GB / Logs per Day		none	COTS	Annual subscription
Fortinet	Forti Gate	Unified Threat Management Protection + Forti Care 24 x 7 (8 devices)		none	COTS	Annual subscription
Fortinet	Maintenance	Annual Software\Hardware Maintenance		none	COTS	Annual subscription
DellEMC	VPLEX	Metro, GeoSync,		none	COTS	Annual subscription
DellEMC	UniSphere	For File, For VMAX, For Power Max, For Unity		none	COTS	Annual subscription
DellEMC	CMCNE	Connectrix Manager		none	COTS	Annual subscription

Dell EMC	Maintenance	Annual Software\Hardware Maintenance		none	COTS	Annual subscription
ServiceNow	ServiceNow	Fulfiller licences		none	COTS	Annual subscription
Dynatrace	Dynatrace	Application performance monitoring DEM		none	COTS	Annual subscription
Dynatrace	Dynatrace	Application performance monitoring HU		none	COTS	Annual subscription

2. Third Party Software

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or NonCOTS)	Term/ Expiry
PRS (Practitioner referral system)	Atos	Core application	Multiple	None	1	NonCots	Annual subscription
SAMS Siebel Appointment management system	Atos	Core application	Multiple	None	1	NonCots	Annual subscription
MIS (management information system)	Atos	Core application	Multiple	None	1	NonCots	Annual subscription

75 words

4.3p)	Data Archiving & Purging	Weighting 0.30% Aesthetic and Functional Characteristics
Guidance:		
<p>The system must be capable of supporting the Buyer's Information Management Policy and GDPR policy. This requirement is not required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, in your response describe if your solution has a built-in archiving functionality that could be configured based on the business rules (e.g. retention period, type of referral)? If there is no built-in functionality, describe how this requirement could be fulfilled i.e. via custom script, tools etc. Is there Functionality to purge the archived data based on the business rules (retention period, type of referral.)? Additionally, describe how your solution;</p> <ul style="list-style-type: none"> • Archives any data that is not actively used • Retrieves archived records back to the live service 		
<p>We confirm that our solution fully meets the Non-Functional Requirement for data archiving and purging, and that as this requirement is already in place for the current solution, it will be included within the for Viable Product Release and by the Operational Service Commencement Date. For the proposed solution, data is stored in two main areas:</p> <ol style="list-style-type: none"> 1. OLTP (Online Transaction Processing) data <ul style="list-style-type: none"> • The Patient Referral System (PRS) and Siebel Appointment Management System (SAMS) databases are the main OLTP databases • PRS is a proprietary case management database • SAMS is a Siebel database used for resource management and appointment booking data 2. OLRP (Online Analytic Processing) data <ul style="list-style-type: none"> • The Management Information Systems (MIS) database is the reporting database where data is automatically uploaded on a nightly basis from PRS and SAMS. • The MIS database performance is less sensitive to actual data volumes and archiving of data is only performed if needed. <p>No master or integral reference data will be archived. Only transactional data that has met the pre-defined criteria will be archived. All archived data will be secured as read-only. Provided the referral is fully processed and no longer active, all data purging is subject to GDPR compliance. GDPR compliance for MIS data will be less stringent due to its anonymisation and pseudonymisation of the data for reporting purposes only.</p>		

All archiving and purging tasks are performed through predefined stored procedures run on a daily basis. These stored procedures can be configured to alter retention periods for all or specific referral types. These tasks are run during off-peak, specified maintenance windows to avoid competition with normal application processing. Detailed change management practices govern change requests, not only to applications and databases, but also archiving and purge procedures to ensure archive, retrieval and purge processes are considered as part of any application updates.



Operational stability
and security

The Buyer can be assured that one of the key themes of our solution is operational stability and security and through the continuation and enhancement of the current our proposed solution fully delivers this objective.

336 words

4.3q)	MI, Data and Analytics	Weighting 0.30% Aesthetic and Functional Characteristics
Guidance:		
<p>The Buyer would like to understand how your solution can support accurate Management Information data for consumers, both the Buyer and Healthcare Providers.</p> <p>Please also include details on any user configurable MI services (e.g. user driven reports) or API's available for MI data which form part of the overall solution and how these could be used by both parties.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
Incorporating the guidance above, your response should detail MI reporting capabilities and functionality.		
<p>Introduction</p> <p>We confirm that our solution fully meets the requirement for MI, Data and Analytics in alignment with attachment 6.1 milestones. It will be delivered for the Operational Service Commencement Date.</p> <p>MI Reporting</p> <p>Our solution will extend the reporting database employed to deliver Management Information(MI) requirements for the AIS service and provide both current and bespoke reports to the area of the business requiring the information, or giving access through a reporting tool to the end user allowing them to produce their own queries and reports.</p> <p>To create the MI solution, packages have been developed to extract, transform and load data (ETL) from the operational systems PRS and SAMS into an Enterprise Data Warehouse (EDW). The scheduling of the ETL packages extracting and loading the data from the systems is related to the timeliness requirement of the business need. Jobs update every 10 minutes, 30 minutes, hourly and daily dependent on how up to date areas of the business require information.</p> <p>The EDW currently contains over 40 Data Marts where the data is integrated giving the whole picture on a business area and in an aggregated format suitable for reporting on at the level required by the business and allowing for data to be presented with differing levels of granularity. This allows for reports to run quickly with accurate business ready output. The number of data marts can be increased to better fit areas of the business if the need is identified.</p> <p>Reports produced will fulfil the functional requirements specified by the buyer and allow for filtering, drill through and drill down functionality. There are 32 reports specified in the functional requirements and these may be split into separate reports.</p> <p>The MI data needs of the Buyer are currently met with the provision of bespoke reports designed and developed to the Buyer's requirements. The plan is to enhance functionality within the Buyer's organisation and to extend it to Healthcare Providers by giving licensed Cognos reporting tools to certain individuals enabling them to directly access the MI database to produce their</p>		

own queries and produce ad hoc and scheduled reports in addition to any provided by Atos. This facility is planned for delivery as part of work package 8 and will be available for Viable Product Release.

With access granted to users across different areas of the business and across different Lots, security will be in place so that users can only see information pertaining to their Lots and the area of the business where they have a need for access. Roles will be created ensuring that all users can only see the data that they have a business need to access.

Users with access to the MI database will be given training using the reporting tool to able to create their own reports and queries enabling them to extract the MI information they require.

474 words

4.3r)	Usability	Weighting 0.40% Aesthetic and Functional Characteristics
Guidance:		
<p>The Buyer would like to understand how your solution can ensure the effectiveness, efficiency, and satisfaction of the users when using the service / component to achieve their business goals.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should detail how your solution ensures:</p> <ul style="list-style-type: none"> • Optimal Completion rates • Minimal Time to complete • Minimal Error Rate • Reduced Training Cost • User Satisfaction 		
<p>Our solution fully meets the Buyer's requirements for optimal completion rates, minimal time to complete/error rates, reduced training costs and user satisfaction. It will meet or exceed these requirements both for Viable Product Release and for Operational Service Commencement.</p> <p>Completion rates HP utilisation and productivity are paramount to business delivery. To support management and control, HP diary and rota functionality is inbuilt showing working hours and daily workstream allocation. Our solution offers 'intelligent scheduling', which applies statistical weightings to categorise consultations by expected duration. This balances HPs' daily workloads and reduces appointment cancellations. Our solution maximises utilisation by allowing HPs to self-serve appointments on demand from pooled over-bookings, which triggered an immediate uplift in HP utilisation when introduced. The assessment-writing function is optimised for efficiency and is integral to the case management system rather than a standalone component, providing a seamless experience for HPs.</p> <p>Minimal time to complete Speed of case progression is inherent across the solution design. For example, work is routed automatically into appropriate 'get next' queues from which users self-select the highest priority task available. Clinical audit selection is also performed instantly on report submission.</p>		

The automatic appointment booking provided by our solution has greatly flattened regional peaks and troughs of aged cases through virtualised appointments, automatically booking oldest cases into the next available slots regardless of geography, protecting the claimant experience by optimising time to complete across a given provider's geography.

Minimal error rates

Error rates are kept to an absolute minimum through extensive validation and business rules throughout the applications. A state model is enforced by the integrated jBPM workflow engine which only enables specific activities to be undertaken at appropriate times in the process.

Users are supported in producing high quality assessment report content by a context-sensitive phrase-builder which limits errors of omission; completed assessment reports are screened for other potential errors by the risk-based audit rules engine, which has proven to be 10-15 times more effective than quality checking a random sample.

Reduced training costs

Approximately 70% of the existing AP user-base is already highly proficient in the use of our proposed solution. Our transition plan involves the incremental deployment of functional enhancements into production for these IAS users, during which training increments will be minor and be complete by Viable Product Readiness. Only the current Capita user-base will then require training, keeping overall training costs to an absolute minimum.

User satisfaction

Atos has ensured user satisfaction by co-designing the solution with its HPs, many of whom brought years of experience collaborating with the Buyer's clinical advisory teams and conducting assessments across a range of benefits.

We have demonstrated our committed to user satisfaction through continuous investment in service improvements since the inception of PIP. This will benefit all APs as our solution fully retains this investment. The Atos team has the detailed knowledge and experience to help the Buyer and its PIP assessment providers identify and drive through further improvements on an ongoing basis through collaborative engagement to deliver creative solutions.



499 words

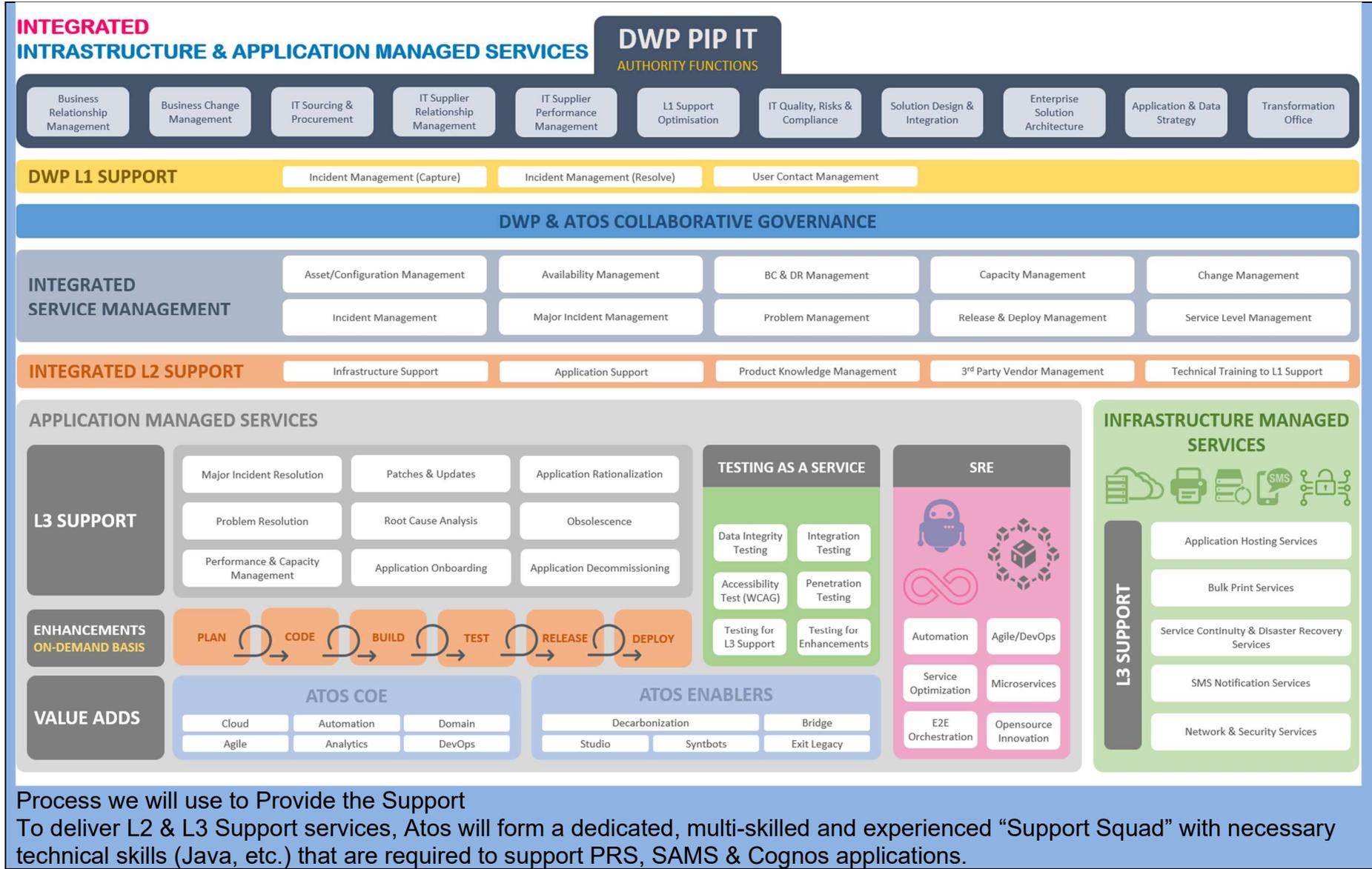
4.4 Non-Functional Requirements (Service Management Requirements) – 5%

4.4.1 The Non-Functional Requirements (Service Management Requirements) of the Buyer are listed in questions 4.4 below.

4.4.2 For each of the Non-Functional Requirements (Service Management 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).

4.4.3 Please see the Further Competition Instructions to Bidders paragraph 22.16.5 for the Non-Functional requirements (Service Management Requirements) detailed evaluation information including the marking scheme used for all of the questions in this section.

4.4a)	Error / Problem Resolution	Weighting 0.40% Technical Assistance
Guidance:		
<p>The Potential Provider must provide, second and third line Level support to fix errors or problems with the solution, so that it operates in accordance with its design and documentation. First line support will be provided by the Buyer This requirement is not required for Viable Product Release (See Attachment 6.1) This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should detail how this requirement can be met. This could be in the format of text and/or a diagram and should include the scope, processes and hand-off points between first line support, second line support and third line support.</p>		
<p>Introduction We confirm that our solution fully meets the requirement for Error & Problem Resolution and that as this requirement is already available by the Operational Service Commencement Date. Our solution will provide a scalable model incorporating L2/L3 Support, Agile Development, Testing as a Service (TaaS) and Site Reliability Engineering (SRE); Atos will accelerate the delivery of the Buyer's journey, achieving best-in-class end user satisfaction, and collaboration across the IT service ecosystem. Our solution will provide an intelligent, self-healing application service, delivered through smart, industrialised capabilities, and supported by cognitive AI and automation to drive operational efficiencies.</p> <p>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. This approach will ensure that the systems are fully onboarded and ready for operational service, starting from 1st March 2023, as detailed in our Implementation Plan.</p>		





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] FOIA S43 Commercial Interest . This approach also supports the Buyer’s “fix first” culture requirement to reduce its management overhead.

Added Value: We will introduce [Redacted] [Redacted FOIA S43 Commercial Interest] for driving Continual Service Improvements (CSI) including process improvements, elimination of waste and automation leading to improved efficiency, increased pace of change and enhanced quality all leading to improvements in Buyer’s end user experience and reduce the operational costs. [Redacted] [Redacted FOIA S43 Commercial Interest]

Our “TaaS” 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.

498 words

4.4b)	Support and issue resolution	Weighting 0.40% Technical Assistance
Guidance:		
<p>The Potential Provider must be on-boarded to the Buyer Incident Management Reporting tool DWP Place (Service Now) and the Potential Provider must work with the Buyer on reported issues through to successful resolution within the agreed service level agreements and Key Performance Indicators.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>		
Question:		
<p>Incorporating the guidance above, your response should detail:</p> <ul style="list-style-type: none"> • Your requirements for on-boarding to DWP Place. • How you can work with the Buyer on reported issues through to successful resolution 		
<p>Requirements For Onboarding To DWP Place</p> <p>We confirm that our solution meets the requirement for Support & Issue Resolution, and that as this requirement is already available within the IAS operations, it will be included within the Viable Product Release and by the Operational Service Commencement Date.</p> <p>Atos has experience in onboarding service operations to ServiceNow for many clients including [REDACTED] Redacted FOIA S43 Commercial Interest</p> <p>Incidents, SRs and CMDB on the IAS platform are handled using ATF ServiceNow, hosted on the IRIS platform. To onboard the service operations to DWP Place, Atos plans to implement a Data Gateway integration between “DWP Place” and “ATF ServiceNow” during the implementation phase to sync the incident data between the systems. Incidents created and assigned in “DWP Place” by L1 support will reflect in “ATF ServiceNow” for L2 or L3 support. Status updates made for an incident by L2 or L3 support will immediately reflect in “DWP Place” to enable L1 support track the incident for closure. Service Request (SR) & CMDB will be handled manually between the systems.</p> <p>Our requirements for on-boarding to DWP Place:</p> <ul style="list-style-type: none"> • Only incidents are considered for Data Gateway integration • Buyer’s “Adapter Standard” will be considered for Data Gateway integration • ATF ServiceNow CMDB will have enough information to be able to achieve ticket tagging; majority of the CI details will be present in DWP Place • ATF ServiceNow CMDB & Service Request will be updated manually • Data Gateway interfaces will be configured via Atos Standard Integration method 		

- Buyer will be responsible for “DWP Place” and its corresponding interface development and configurations
- Development and configuration of the portal and catalogue items on DWP Place is Buyer’s responsibility
- Enabling of ports / protocols / service accounts on the target servers
- Configuration of prerequisite workgroup, SLA, required workflows in DWP Place (for interface integration) is Buyer’s ownership
- Migration of tickets (Incidents & Service Request) is not considered
- It’s not possible to request changes to ATF ServiceNow (ZERO-change policy) or provide direct access to ATF ServiceNow CMDB.

Successful Issue Resolution

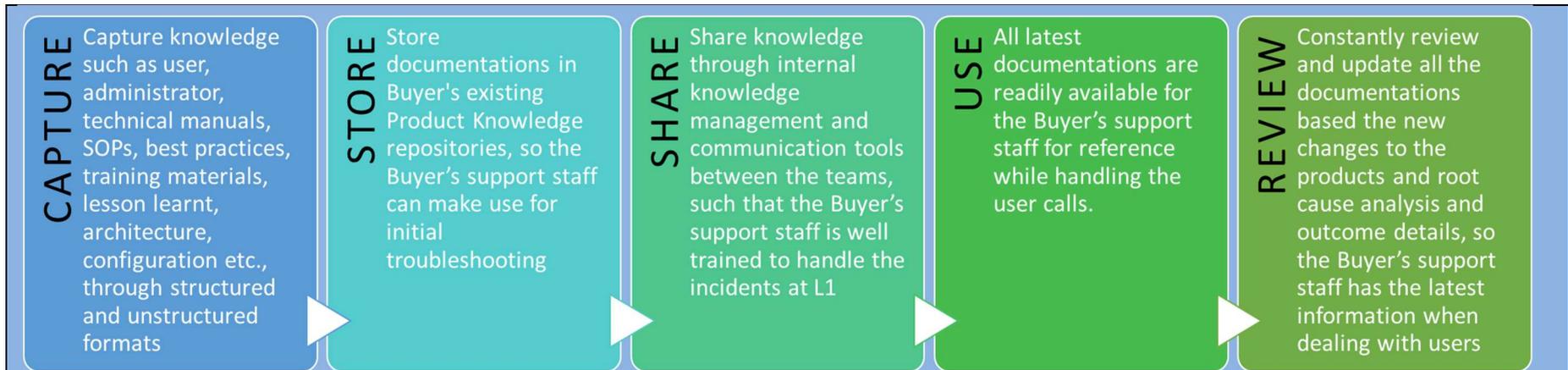
Our Issue Resolution Process includes six logical steps to assist the Buyer. Issues are continuously assessed, monitored, and actively managed until they are resolved or turned into problems.

1. Identify: We work with the Buyer to identify the issues
2. Analyse: Conversion of an issue into a form that facilitates decision-making. Issue prioritisation ensures the most important issues are prioritised and handled first
3. Plan: Use the outcome from issue analysis and use it to formulate strategies, plans, and actions. Issue scheduling ensures plans are approved and then incorporated into the day-to-day Service Management process
4. Track: Monitor the status of issues and the progress in their respective action plans
5. Control: Execute action plans and their associated status reporting. Outcome from this stage will be a status report that documents the progress towards the resolution of the issue
6. Learn: Formalises the lessons learnt and captures the knowledge in reusable form to be used within the service.

493 words



4.4c)	Documentation Weighting 0.40% Technical Assistance
Guidance:	
<p>The Potential Provider must provide all product knowledge documentation (including Administrator, Technical, Configuration, Users) to the Buyer support staff, for initial troubleshooting.</p> <p>The Potential Provider must provide regular service performance reports</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail:</p> <ul style="list-style-type: none"> • The scope and outline content of the product knowledge documentation • How the documentation can be delivered to the Buyer support staff • How you can work with the Buyer to support initial troubleshooting. • The method, scope and frequency of service performance reports 	
<p>Documentation / Product Knowledge Management</p> <p>Our solution fully meets the requirements of Product Knowledge Management and will be included by the Operational Service Commencement Date. Given our solution is based on the IAS services this is already in a mature state.</p> <p>We have developed robust Knowledge Management (KM) processes and tools that enable a suitable knowledge sharing environment and culture for our customers. Our KM approach for the Buyer's Support Staff will be focused on the following:</p> <ul style="list-style-type: none"> • Fostering a knowledge sharing culture • A single system for capturing and storing product knowledge • Accurate, reliable, up-to-date, and version-controlled product knowledge assets • Ensure continual planning for knowledge enhancement • Information is available at the right time for initial troubleshooting • Metrics captured to ensure the effectiveness and usability of knowledge. <p>The figure illustrates our KM approach for Capturing, Storing, Sharing, Using & Reviewing the knowledge. Our L2 Support will be responsible for maintaining and updating the product knowledge documentation:</p>	



Our Service Management team will organise monthly “Reverse Engineering” workshops to analyse the number of incidents routed from L1 Support to L2 Support. The documentation gaps will be identified and fixed; required knowledge and updated documentation details will be shared with the Buyer. As this is an important aspect of knowledge sharing, we have implemented this approach in most of our customer engagements, e.g., [Redacted] Redacted FOIA S43 Commercial Interest. We will bring this experience and best practices to the Buyer.

Service Performance Reporting

Design: During the implementation phase our Service Design team will design the service performance reporting to measure the KPIs defined in Schedule 2.2 (Performance Levels) and seek approval from the Buyer before the operational commencement date. The team will also define the process for measurement of KPIs, as well as the process for monitoring and improving the service performance.

Method: We will use “DWP Place” for the delivery of all the ITIL processes as a single system of record. This will enable us to provide on-demand Performance Reporting and data extracts for the KPIs. Service Management team we will conduct audits on quarterly basis of the aggregated performance data held in “DWP Place”. The results of any such audits will be published to the Buyer upon audit completion.

Frequency: Service Management team will produce the performance reports on monthly basis and will be added to the Monthly Service Report. This will be shared with the Buyer within 5 Working Days of the end of each service period.

Review: The team will review the format of the KPI information on a quarterly basis and agree any revisions with the Buyer, before implementing any required changes in the subsequent service period. We are accustomed to adapting the content, format and style of performance reports, service maturity and business demand changes over the life of a contract. We will use the “Performance Analytics” module of the ServiceNow to provide dashboard views, drill-down capability for monitoring, management, and reporting as shown in the sample image below.

Maximum 500 words

4.4d)

Fixes

Weighting 0.40%
Technical Assistance

Guidance:

The Potential Provider must provide fully tested, supported and documented hotfix/patches with installation guidelines and regression test procedures.

This requirement is not 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 scope of testing to be carried and what evidence can be provided to support assurance and sign-off
- Outline content of the hotfix/patches with installation guidelines and how this can be assured prior to release and deployment into the relevant environment

Introduction

We confirm that our solution fully meets the Requirement for Fixes and that as this requirement is already being delivered within our operations for the current PIP service, this will be included for Viable Product Release and Operational Service Commencement Date.

Hotfix/patch testing

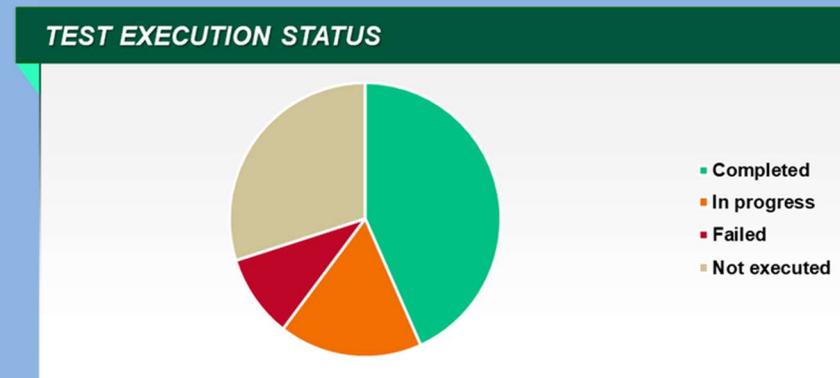
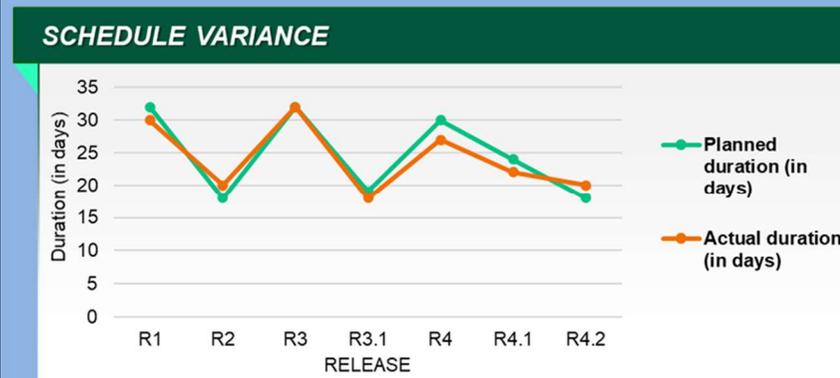
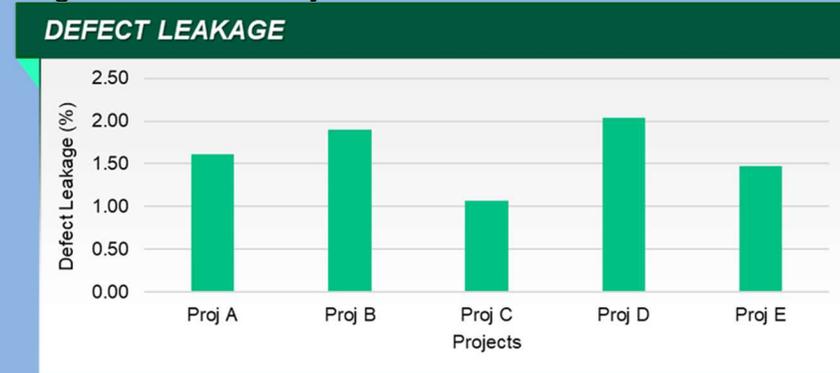
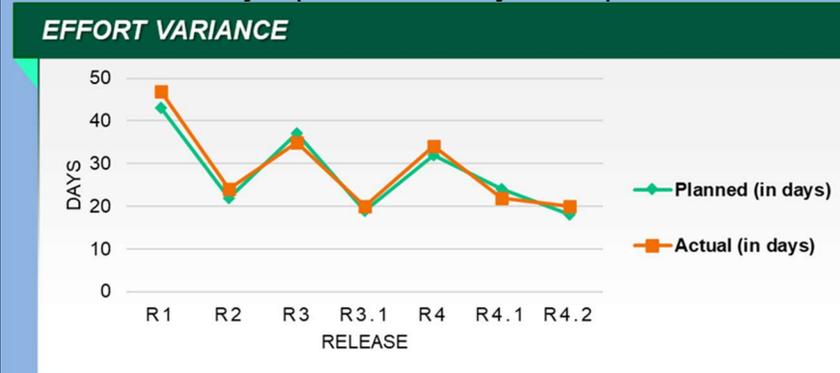
When the QA team gets the Hotfix/patch, they will prepare tests to validate Hotfix/patch specific functions. As part of test preparation, the team will define test scenarios and test cases. The team will also work on test pre-requisites, data and environment pipe-clean tests to ensure readiness for Test Execution.

In parallel, the QA team will analyse the impacted functionalities and plan for regression testing with installation guidelines and regression test procedures. Regression testing will take place after a code release to confirm the quality and integrity of the build. Regression Testing will include targeted testing of code being changed. In order to ensure the regression tests are targeted correctly, analysis will be performed with the development teams, to understand the affected components and the level of risk. When the hotfix contains a major change, then full regression test pack will be executed.

As part of test automation, the QA team will undertake a feasibility assessment and select the potential test scenarios/cases for automation based upon technical feasibility and frequency of execution. Atos will leverage our in-house web-based automation framework for scripting the web-based scenarios, creating automation scripts.

We will define a list of testing metrics and a Hotfix test reporting template to track as part of this engagement.

At the end of the testing phase, the QA team will prepare a detailed test summary report covering the number of test cases along with test results, regression pack details (with list of modules covered) and defect summary etc. The team will submit the test summary report after every hotfix/patch release and get sign-off from the Buyer.



We perform similar patch testing services for a global document technology corporation. Our testing team execute functional and automated test cases for frequent patches/upgrades and have adopted DevOps testing to speed up the testing deliverable by up to 90%.

Hotfix/patch content

All hotfix/patches, including code changes, bug fixes, configuration changes and other applications changes will be identified, assessed, and applied using Change Management governance to ensure impacts are identified and mitigated. When a new hotfix is made available, our Technical, Functional & Test Leads will implement the testing without affecting the business. Depending upon the extent of change, our Test Lead will organise an advance testing to ensure we have all the information necessary to help the Buyer make an informed decision about applying the hotfix/patch. The configuration management

process will ensure that the Definitive Media Library (DML) and the Configuration Management Database (CMDB) is updated with current information including details of new/changed application objects.

"We provide application support services to several customers like [REDACTED] Redacted FOIA S43 Commercial Interest, where it includes providing services such as hotfix/patches. We will bring this experience and best practices to the Buyer."



Operational stability
and security

488 words

4.4e)

Contact details

Weighting 0.10%
Technical Assistance

Guidance:

The Potential Provider must provide a named UK based account manager for escalations.
This requirement is not 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 details of:

- A named UK based account manager, demonstrating their account manager skills and experience in dealing with an account of this size and scale.

The Atos account team will be led by [REDACTED], Client Executive Partner. As detailed below, [REDACTED] has extensive experience in this role in a similar context. He meets all the requirements for the position in full and will be available to start in advance of Operational Service Commencement Date.

[REDACTED] has 10 years of experience with Atos as a senior Account Executive with major clients. In that time, he has been responsible for the delivery of large IT Managed Service contracts with [REDACTED]

[REDACTED] Importantly, [REDACTED] experience has included both complex transitions and critical service delivery. In these roles he has been accountable to the Atos UK Board and the relevant Client SROs for all aspects of Atos delivery including the suitability and performance of senior Atos personnel, service level and project/programme achievement, compliance with relevant regulations, customer satisfaction and maintaining the commercial integrity of the contract.

To achieve these challenging objectives, [REDACTED] has used his personal expertise and industry knowledge, built up over 19 years working in the IT industry, and the leadership capabilities which he developed during his previous 13 years of service as [REDACTED]. In addition to his strong technical, management and leadership skills, [REDACTED] has a superb track record in establishing trust with senior Client counterparts and developing partnership and governance models that enable clear, open discussion and rapid resolution of issues, as well maintaining a focus on improvement, innovation, and support for future strategy. In addition, he has successfully built account-level supply chain relationships with vendors and hyperscalers, including Dell, Citrix, IBM, Microsoft, AWS & BT, to ensure they deliver high-quality support and maintain accountability. As Client Executive for [REDACTED] used his experience and professional abilities to motivate and inspire the long-serving team to improve performance and proactively support the Client through challenging organisational change programmes.

For DWP, [REDACTED] will implement a proven account management organisational structure, using his experience with Clients such as the [REDACTED], where Atos's service provision is similar in scope. Using this approach at [REDACTED].

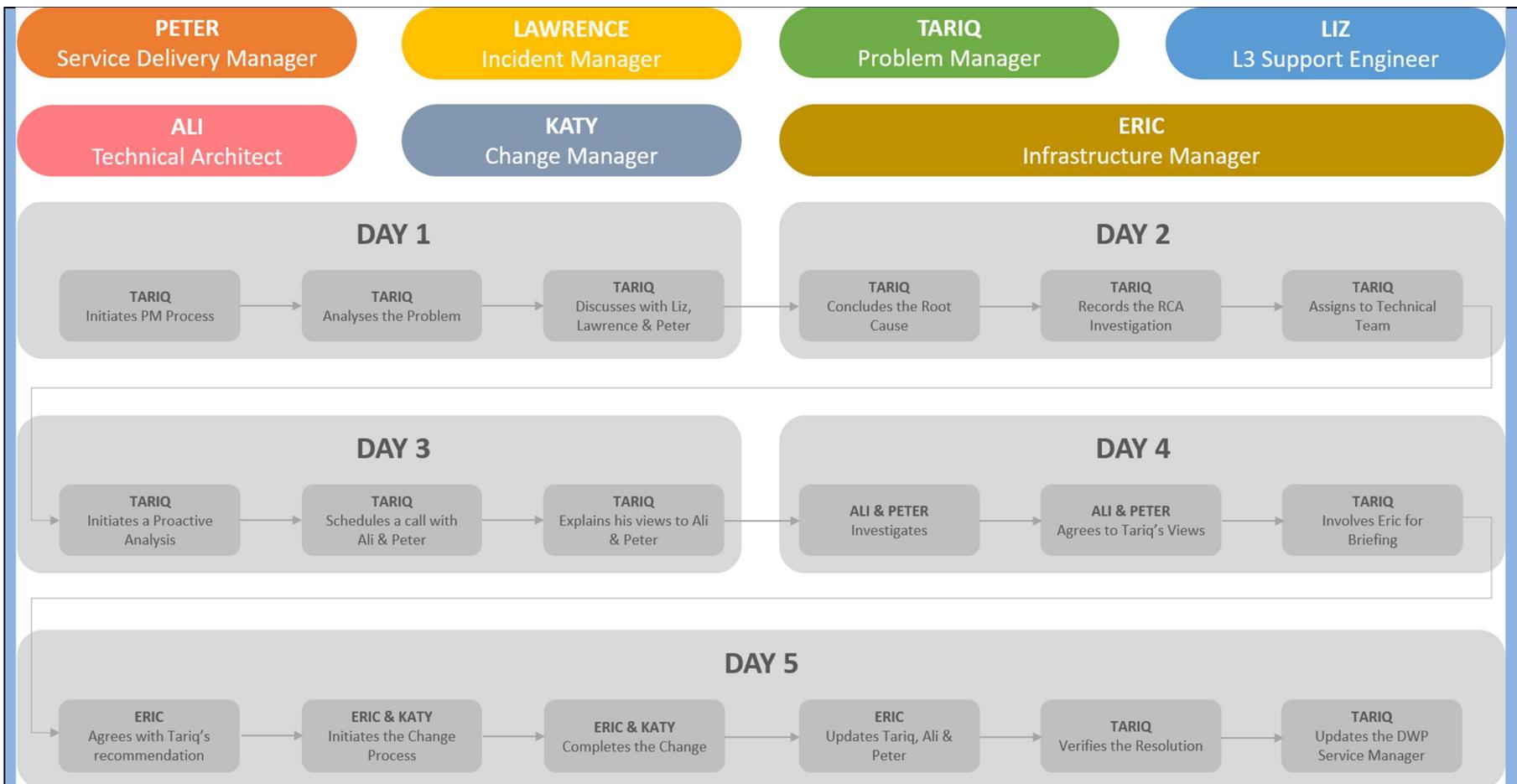
. enabled a newly-established Atos team to come together quickly and transition all clinical and administrative IT services from a previous incumbent to Atos management, tooling and support at very short notice with no interruption to live service which was a clinical imperative. The account team structure will also incorporate experienced personnel from the existing DWP support team, where appropriate, and link seamlessly with our other DWP service provision.

██████ is a passionate advocate within Atos for social value. He is Chair of one of our Diversity & Inclusion networks and recently led the successful campaign to revalidate our Armed Forces Covenant Gold Award status. ██████ will provide DWP and the Atos account team with the leadership, direction and support to ensure that transition, live service and future transformation are delivered successfully.

Redactions FOIA S40(1) Personal Details and S43 Commercial Interest

496 words

4.4f) Root Cause Analysis	Weighting 0.40% Technical Assistance
Guidance:	
<p>The Potential Provider must provide root cause analysis reports, within 5 calendar days of resolving a Priority 1 incident related to the production solution.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your solution response should detail:</p> <ul style="list-style-type: none"> The scope, outline content and process for meeting this requirement 	
<p>We confirm that our solution fully meets the requirement for Root Cause Analysis (RCA), and that as this requirement is already available, it will be included by the Operational Service Commencement Date from when Atos will provide RCA reports within 5 calendar days of resolving a P1 incident.</p> <p>Scope</p> <p>Reactive Problem Management: When a P1 incident is resolved a problem record is created and the Incident Manager will involve the Problem Manager (PM). When the problem remediation activities are identified, the PM will liaise directly with the Change Manager to ensure they are aware of the required activities for resolving the related problem record.</p> <p>Proactive Problem Management: PM will use “DWP Place” to perform trending analysis on incidents to diagnose issues using techniques like 5 Whys or a Fishbone Diagram. Preventing or minimising the impact of incidents, through implementing effective workarounds, preventative actions, and permanently fixing the root cause of the problems, will contribute directly to keeping the PIP IT services operational.</p> <p>Process</p> <p>The diagram below shows our approach to proactively manage problems.</p>	



[DAY 1] Following the resolution, the incident details are passed to Tariq to initiate a Problem Record and begin to perform the RCA. The problem investigation will follow the process as defined in the Problem Management process.

[DAY 1] Tariq analyses the incident by going through the logs, the events that occurred from identification to resolution, and arranges a call with Liz, Lawrence, and Peter to determine the actions that were taken leading to the resolution of the incident.

[DAY 2] After the RCA, it is concluded that due to the incompatibility of the hardware that was brought in and the coding in the database caused the incident. It is also investigated if the change should have been backed out, and it is agreed that due to the unavailability of additional hardware, the change made to the database to re-route traffic was the right call. Tariq records the details of the investigation and root cause within the Problem Record in "DWP Place" and assigns actions to the relevant technical owners to ensure prevention / mitigation of further impact.

[DAY 3] Tariq then moves into pro-active mode, where he analyses the reports produced against Configuration Item (CI), looking at the “top talkers” (i.e., the CIs with the most incidents against them). Tariq then works with Ali and Peter to determine that – to reduce the volume of incidents moving forward, a hard drive issue should be investigated on a server because there were several incidents logged due to a hard drive failing multiple times.

[DAY 4] Tariq engages Ali and Peter to investigate and they both concluded that hard drive should be replaced. Tariq gets in touch with Eric and runs him through the recommendation with the justification that it has the potential to prevent approximately 30 incidents a month and an unspecified amount of unplanned outage to the system.

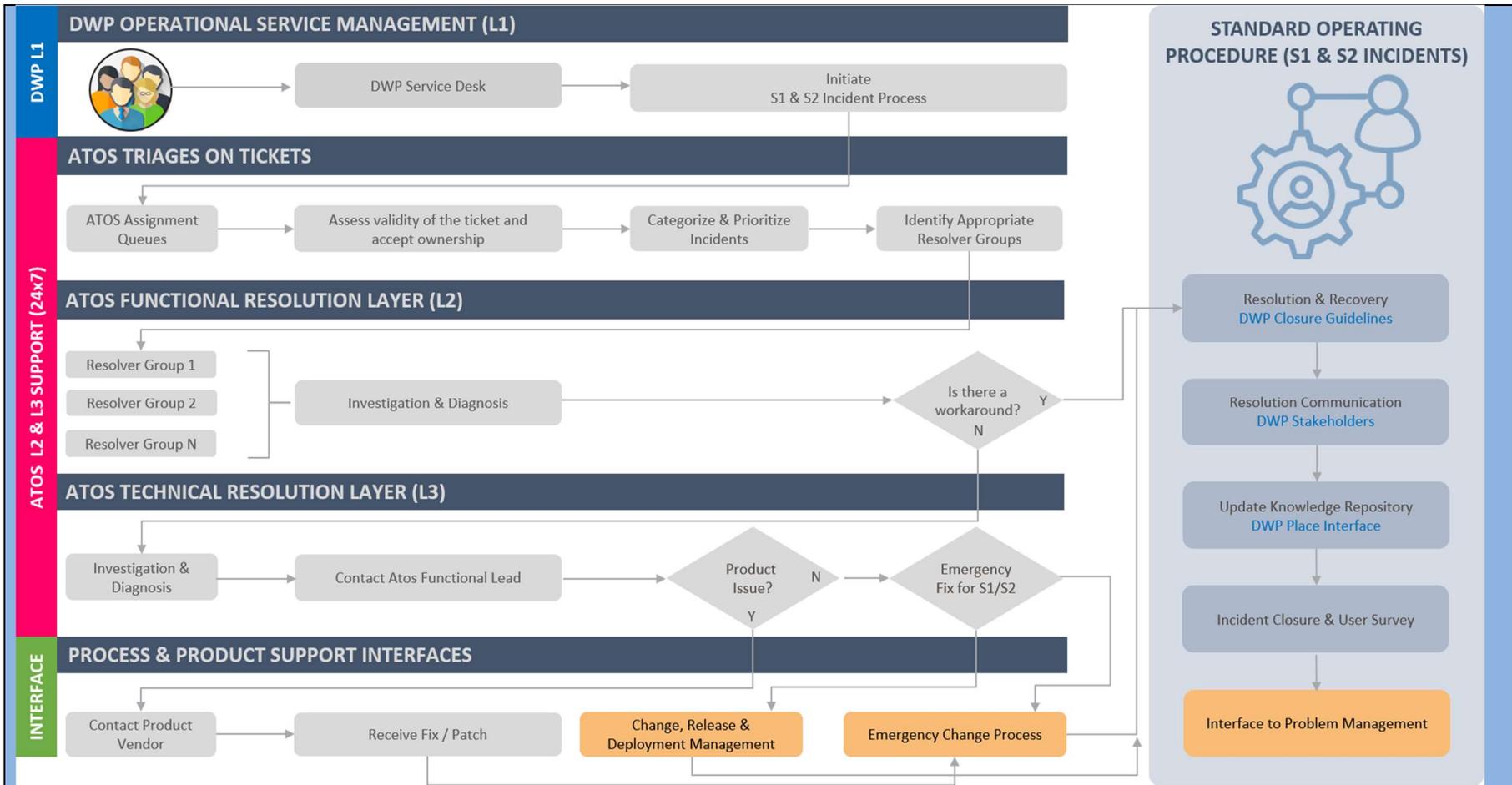
[DAY 5] Eric takes the recommendations on board and arranges to swap out the hard drive through the change process.



Operational stability
and security

498 words

4.4g) Support Times – Severity 1 & 2	Weighting 0.40% Technical Assistance
Guidance:	
<p>The Potential Provider must provide UK based support 24 hours, 7 days/week, 365 days/year for Severity 1 & 2 incidents. (See table below for severity definition).</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your solution response should detail:</p> <ul style="list-style-type: none"> • How this requirement can be met • How ongoing changes can be communicated to the Buyer 	
<p>Our solution fully meets the requirement for Support Times – Severity 1&2, and these support capabilities will be included by the Operational Service Commencement Date (given our solution is principally based on a continuation of our current provision, which exists today.)</p> <p>Resolving S1 & S2 Incidents</p>	



To support the resolution of S1&S2 incidents, we will implement and operate an Incident Management (IM) function. Our IM function consists of five sub-areas:

- Incident Registration & Initial Support
- Incident Triage, Diagnosis & Resolution
- Incident Closure & Knowledge Update
- Incident Tracking, Escalation & Communication
- High Priority Incident Management.

To provide daily support, Atos will deploy Teams 1&2, who will be available on a rota-based shift pattern. Using this model means that there is flexibility to increase effort in line with higher demand windows (as shown below). Team 3 will operate on an on-call basis and cover the out of hours support. All 3 teams will be UK-based, providing 24 hours, 7 days / week, 365 days / year support.



Demonstrating our Procedure

MATTHEW End User (DWP)	ERIC Infrastructure SDM	AILEEN Service Desk Agent (DWP)
LAWRENCE Incident Manager (Atos)	LIZ L3 Support Engineer (Atos)	PETER Service Delivery Manager (Atos)
ALI Technical Architect	MARKUS Infrastructure Manager, Servers	KATY Change Manager (Atos)

1. Matthew is unable to access a PIP application at 9:30. He speaks to Aileen on the Service Desk and advises Aileen this is a critical application. Aileen registers the incident as S1 or S2
2. Lawrence advises Aileen that investigations are under way and to keep an eye on the ticket, as he will add updates in ServiceNow as they become available
3. Lawrence arranges a call with Liz, Ali, Eric, Peter. Liz, Ali advises that they are currently reviewing the logs and are close to identifying the issue. Eric advises that he provides an update to stakeholders, Lawrence updates the incident. It is decided that Liz and Ali need a further 25 minutes to identify the issue; so, it is agreed to reconvene the call in 30 minutes at 10:30
4. Liz and Ali continue investigations and determine that a change performed overnight to swap some hardware has introduced a routing error within the database
5. Eric requests Markus joins the 10:30 call to discuss if the change should be reverted. It is decided that the impact of reversion will be greater than to fix the forward impact; so, it is agreed that Liz will raise a Change to amend the hardcoded routing instructions in the database and engages Change Management to raise an Emergency Change
6. At 11:00, Matthew checks for the latest update and can see an update from Lawrence that the issue has been identified and a Change is being raised and is scheduled for 11:15 pending all approvals
7. Matthew logs back at 11:30 into the application and is delighted to be able to access all functions as expected and informs Lawrence that everything is working
8. Lawrence checks with Matthew if there are any other areas, where he thinks the user experience could be improved
9. Lawrence gets similar confirmation from other affected users that it's working. He closes the incident and issues an incident resolution communication to the defined communications list.



496 words

4.4h)**Severity Times – Severity 3 & 4****Weighting 0.40%
Technical Assistance****Guidance:**

The Potential Provider must provide UK based support during Operational hours of business for Severity 3 and 4 incidents. (See table below for severity definition)

Note: Operational Hours are 8am-8pm weekdays and 9am-5pm on Saturdays and Sundays.

This requirement is not 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 solution response should detail:

- How this requirement can be met
- How ongoing changes can be communicated to the Buyer

We confirm that our solution fully meets the requirement for Support Times – Severity 3 & 4, and that it will be included by the Operational Service Commencement Date.

Resolving S3 & S4 Incidents

To support the delivery of resolving the S3&S4 incidents, we will use the same Incident Management (IM) function that is setup for S1&S2 incidents but operate with different SLAs as agreed with the Buyer. The IM function will be responsible for managing the lifecycle of all S3&S4 incidents. In this case, our IM function consists of four sub-processes:

- Incident Registration & Initial Support
- Incident Triage, Diagnosis & Resolution
- Incident Closure & Knowledge Update
- Incident Tracking, Escalation & Communication, including the Buyer & Third parties.

To provide 12x5 coverage during the weekdays (12 hours a day / 5 days a week), Atos will deploy Team 1 & 2, who will be available on a rota-based shift pattern. To provide 8x2 coverage during the weekends (8 hours a day / 2 days a week), Atos will deploy Team 1, who will be available on a rota-based shift pattern. Using such model means that there is flexibility to increase effort in line with higher demand window (as shown below). Both teams will be UK-based.



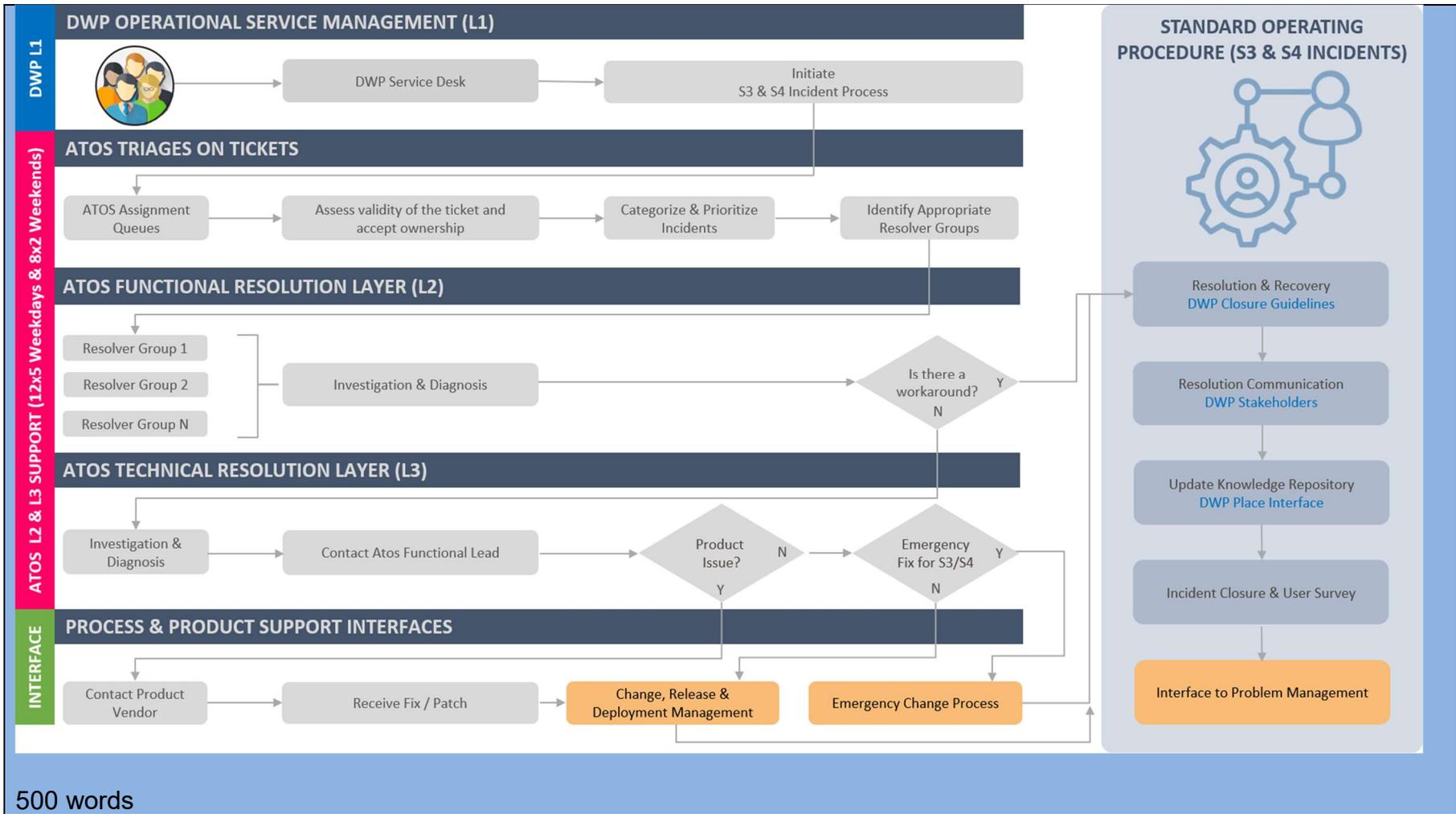
Demonstrating our Procedure

MATTHEW End User (DWP)	ERIC Infrastructure SDM	AILEEN Service Desk Agent (DWP)
LAWRENCE Incident Manager (Atos)	LIZ L3 Support Engineer (Atos)	PETER Service Delivery Manager (Atos)
ALI Technical Architect	MARKUS Infrastructure Manager, Servers	KATY Change Manager (Atos)

1. Matthew is unable to access a non-critical PIP application. He speaks to Aileen from the Service Desk. Aileen registers the incident as S3 or S4
2. Lawrence advises Aileen that investigations are under way and to keep an eye on the ticket, as he will add updates in ServiceNow as they become available

-
3. Lawrence arranges a call with Liz, Ali, Eric, Peter. Liz, Ali advises that they are currently reviewing the logs and are close to identifying the issue. Eric advises that he provide an update to stakeholders and Lawrence updates the incident
 4. Liz, Ali continues investigations and determine that a change performed overnight to swap some hardware has introduced a routing error within the database
 5. Eric requests Markus to join the call to discuss if the change should be reverted. It is decided that the impact of reversion will be greater than to fix forward impact; so, agreed that Liz will raise a Change to amend the hardcoded routing instructions in the database and engages Change Management to raise an Emergency Change
 6. Later, Matthew checks for the latest update and can see an update from Lawrence that the issue has been identified and a Change is being raised and pending for approvals
 7. Following day, Matthew logs back into the application and is delighted to be able to access all functions as expected and informs Lawrence that everything is working fine
 8. Lawrence checks with Matthew if there are any other areas, where he thinks the user experience could be improved
 9. Lawrence gets similar confirmation from other affected users that it's working. He closes the incident and issues an incident resolution communication to the defined communications list.

Below is our incident resolution process for S3&S4 tickets:



4.4i) Security Management	Weighting 0.40% Technical Assistance
Guidance:	
<p>The potential Provider must support the Buyers Security Management responsibilities. This could include: Providing a suitably qualified representative to attend an associated Security Working Group which would facilitate ongoing security engagement between the Potential Provider and the Buyer. Sharing with the Buyer significant vulnerability, or security related issue. Sharing of relevant incident reports or post incident reports, or similar outputs, and any other significant threat intelligence which may be of interest to the Buyer. 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)</p>	
Question:	
<p>Incorporating the guidance above, your solution response should detail how this requirement can be met, expanding on the examples provided.</p>	
<p>Introduction Our solution fully meets the Non-Functional Requirements. The foundations to our solution are inherited from our current services supporting PIP, whilst refining and enhancing those capabilities enabling us to meet the Operational Service Commencement Date. The solution is hosted on our secure IRIS Platform. IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads. Atos will provide a suitably qualified Client Security Manager (CSM) who will fully support the Buyer in the fulfilment of their Security Management responsibilities. Attending a Security Working Group In line with our current service, our CSM will be the point of contact for all security-related matters and will attend the Security Working Group (SWG) to facilitate the ongoing security engagement between the Buyer, Atos and any other service delivery partners. The IRIS UK Platform operates its own monthly SWG which is chaired by a UK based Operational Security Manager. The Buyer's representatives are also invited to attend the SWG meetings. At each SWG meeting, a monthly operational security report is presented which covers security-related topics including security compliance, patching and antivirus status, security incidents, security deltas, security exceptions, security vulnerabilities and threat updates. Platform security deltas and security exceptions require approval by the members of the SWG.</p>	

The CSM will be responsible for the management of the following:

- Responsibility for the ongoing security relationship between the Buyer and Atos and providing advice and guidance on relevant topics, drawing on our experience of providing the current service to the Buyer
- Providing monthly reporting of the status of security and attending the regular security review meetings
- Sharing significant vulnerability and security related incidents
- Responsibility for ensuring that the Buyer is made aware of potential risks and vulnerabilities and management of these to a satisfactorily mitigated state
- Sharing of relevant incident reports or post incident reports and any other threat intelligence of interest
- Responsibility for the management of security incidents and coordination with the Buyer's security representatives
- Ensuring compliance to Buyer and Atos internal security baselines
- Ensuring applicable Buyer and Atos policies, procedures and standards align to recognised industry best practice
- Providing a risk managed approach to making security related decisions that are ratified by the Buyer.

Sharing vulnerability and security related incidents, and other threat intelligence of interest.

Our CSM will act as the main point of contact and coordinator for all security incidents and will be responsible for ensuring that any significant vulnerabilities are security incident is managed, tracked and reported in accordance with the process. and will be responsible for communicating the nature and severity of the incident with the appropriate parties and leading the investigation from an Atos perspective.

This responsibility includes:

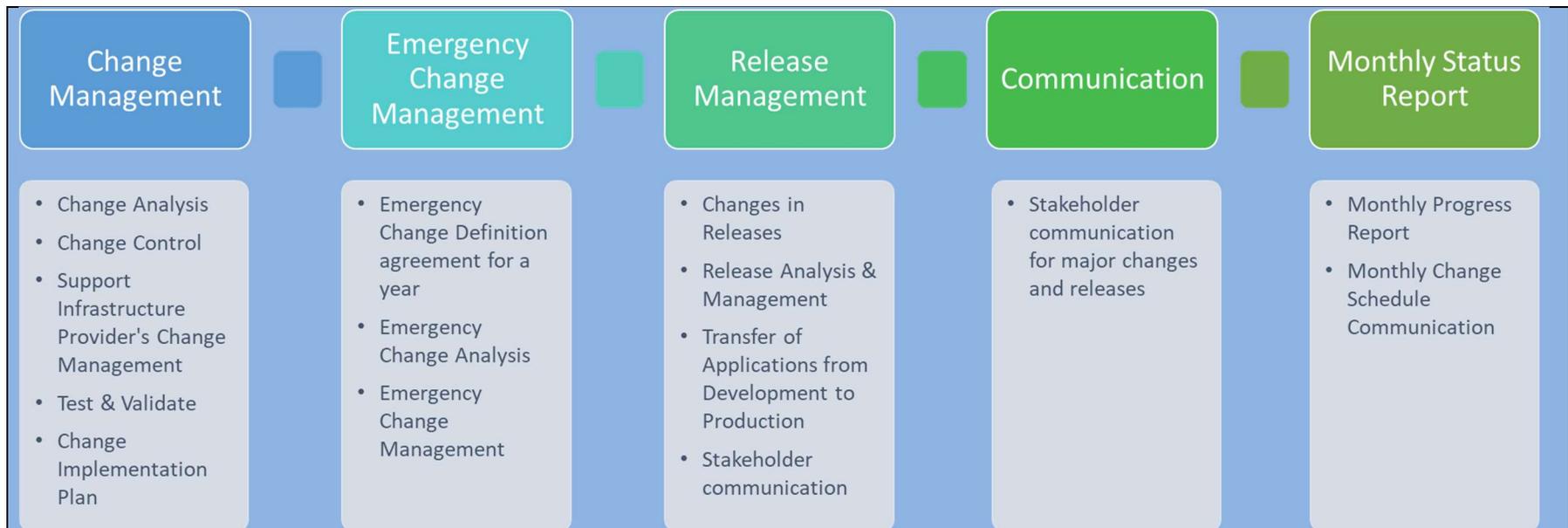
- Sharing significant vulnerability and security related incidents
- S4.2jsharing of relevant incident reports or post incident reports and any other threat intelligence of interest.



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

495 words

4.4j)	Change Management	Weighting 0.40% Technical Assistance
Guidance:		
<p>The Potential Provider must provide a change request and change management process and also align to the Buyer Change Management Processes and Procedures. These should be fully documented and provide a mechanism for responding to the Buyer's request for changes and creating a fully-documented Statement of Work (SoW). 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)</p>		
Question:		
<p>Incorporating the guidance above, your solution response should detail:</p> <ul style="list-style-type: none"> • Your change request and change management process • How it can align to the Buyer Change Management Processes and Procedures. • A mechanism for responding to the Buyer's request for changes and creating a fully documented Statement of Work (SoW). 		
<p>We confirm that our solution fully meets the requirement for Change Management, and that it will be included by the Operational Service Commencement Date.</p> <p>Change Management Process Our Change Management (CM) process will focus on changes to improve business value and end user satisfaction while managing speed, quality, and risk of end-to-end change delivery. The diagram below shows our CM activities.</p>		



Our process provides a mechanism for responding to requests for change and creating a fully documented Statement of Work (SoW). This covers scoping, impact analysis, release planning, design, construction, integration, testing and deployment.

Leveraging experience gained delivering the current services, our team will design an application-specific CM approach/process that will seamlessly integrate with Buyer's defined process during the implementation phase (Apr-2022 to Feb-2023). The process will deliver the following features:

- Change scope and risk tolerance assessment
- Complexity driven impact analysis
- Story point-based estimation techniques
- Automated integration, regression testing, release/deployment
- Automated change workflow, where possible such as approvals/authorisations.

At [Redacted FOIA S43 Commercial Interest], for example, we manage an annual change programme of 100+ projects, 35,000 man-days of delivery have increased efficiency by 300%, whilst reducing time-to-market and risk exposure. We improved Emergency CM process by implementing an efficient impact analysis and review process through a centralised CMDB, release schedules, process, which led to 100% success rate to business. Our proposed approach will bring the same level of proficiency to the Buyer.

To respond to request for changes and create a fully documented SoW; a dedicated Change Manager will be responsible for change co-ordination, governance and adhering to the established processes and standards.

Responsibilities include:

- Allocation of required resources to help generate the Change Implementation Plan
- Ensure relevant pricing for non-standard Change is discussed/approved by Buyer
- Liaise with Buyer to collect any information required to scope the Change
- Drive improvements to the quality of Change, focussing on proactive analysis, reviews, reporting, and lessons learnt from changes that backed out to provide the Buyer valuable insights to help prioritise the change portfolio.

Change Delivery Process

Change Initiation: Our technical team will take up a Change Request as soon as change is approved by the Buyer.

Change Analysis: Our Change Manager, Functional & Technical Lead will assess and review the change scope with all stakeholders to assess the impact of change across all dependencies/CIs including software, components, configurations, customisations, interfaces, data, middleware, batch jobs, and infrastructure.

Change Advisory Board (CAB) Approval: Based on analysis results, our Change Manager will submit the efforts and release schedule to the CAB. After approval, it will be taken for subsequent implementation through a schedule release, as per the proposed timelines agreed with the Buyer.

Change Implementation: Our Change Manager creates a Change Implementation Release Plan, approved by Buyer and regularly provide updates to all stakeholders.

Emergency Changes: It will go-through special approval process defined by Buyer. Emergency changes from S1/S2 incidents will undergo a Post Implementation Review to capture lessons learnt, root cause and proactive measures for avoiding in future.

490 words

4.4k)	Remote Support (Non-Production Dev & Test)	Weighting 0.40% Technical Assistance
Guidance:		
<p>Non-Production (Dev & Test)</p> <ul style="list-style-type: none"> • Configuration for Remote Support incidents must take place inside a designated UK development environment. • RCode production for Remote Support incidents will be subject to the Buyer's security analysis and risk management investigation • All VPN connectivity and setup must be agreed with the relevant Government authorities bound by the Third-Party Supplier. • All connections into the development environment over the internet are to be via an approved secure VPN. • 2-Factor Authentication will be used to authenticate the Remote Support users. • All encryption must comply with the Buyer's Cryptographic Algorithms <p>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691104/dwp-ss007-security-standard-use-of-cryptography.pdf</p> <p>No print/screen print/copy/paste/share capabilities compliant to Buyer standard and policies. 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)</p>		
Question:		
<p>Incorporating the guidance above, your response should detail:</p> <ul style="list-style-type: none"> • How and where in the UK you can provide Configuration for Remote Support incidents. • How you will agree all VPN connectivity and set-up with the relevant Government authorities • How you will obtain approval for secure VPN connections into development environments • How you can incorporate 2-Factor Authentication to authenticate the Remote Support users • How you will demonstrate compliance with the Buyer's Cryptographic Algorithms • How you can ensure there is no print/screen print/copy/paste/share capabilities compliant to Buyer standard and policies. • Initial and ongoing compliance with Remote Support users (Dev & Test) having necessary security clearance • Remote Support users must have necessary security clearance 		
Introduction		

Our solution fully meets the requirements for Remote Support (Non-Production Dev&Test). The foundations to our solution are inherited from our current services supporting PIP, whilst refining and enhancing those capabilities enabling us to meet the Operational Service Commencement Date.

The solution is hosted on our secure IRIS Platform. IRIS UK is our UK Government Secure multi-tenanted Cloud platform supported entirely by UK based SC resources, designed for Official / Official Sensitive workloads.

How and where in the UK you can provide Configuration for Remote Support incidents.

Remote Support for the Buyer's Non-Production is only provided from Atos UK Corporate Devices and the Atos UK Corporate Network via a 'UK Secure Support Zone' hosted on the IRIS Platform.

The Buyer Non-Production Tenant has its own authentication and two factor authentication solution for developers and administrators of the service.

How you will agree all VPN connectivity and set-up with the relevant Government authorities

We will work with relevant Government authorities to agree specific configuration and security parameters for any required VPN connectivity. Our default preference is to configure VPN connections to NCSC's PRIME profile (the most secure profile).

However, if a connecting organisation cannot meet PRIME profile requirements, we will configure the FOUNDATION profile, subject to approval from the Operational Security Manager.

How you will obtain approval for secure VPN connections into development environments

We will work with the Buyer's security representatives and the connecting organisation to seek agreement on the security profile to be used. Any VPN would form part of a documented design and must be approved (from both a technical and security perspective) before implementation.

How you can incorporate 2-Factor Authentication to authenticate the Remote Support users

The IRIS Platform uses two-factor authentication by default to authenticate administrative and user access to the Platform for remote support.

The Buyer Production and Non-Production Tenants have their own authentication and two factor authentication solution for users of the service.

How you will demonstrate compliance with the Buyer's Cryptographic Algorithms

Implementation of the Buyer's Cryptographic Algorithms is an integral part of the solution design.

How can you ensure there is no print/screen print/copy/paste/share capabilities compliant to Buyer standard and policies.

The Gateway Bastion Server at the edge of the UK Secure Support Zone have print/copy/paste capabilities disabled by technical restrictions policy. Screen print and share capabilities are not allowed by policy.

Initial and ongoing compliance with Remote Support users (Dev & Test) having necessary security clearance

A quarterly Security Clearance check identifies personnel whose clearance is nearing expiration and is reported at the IRIS Security Working Group and Client Security Working Groups.

The Non-Production Development and Test environments follow the same security posture as the production environment in terms of Security Clearance, Authentication and secure connectivity.

Remote Support users must have security clearance

All remote support users of IRIS Platform including Buyer Production and Non-Production Tenants are Security Cleared.



Operational stability
and security

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

497 words

4.4l) Remote Support Production	Weighting 0.40% Technical Assistance
Guidance:	
<p>All access to the Production environment will be strictly regulated and controlled. Access to the Production area will only be via Buyer approved locations and devices, and any remote support users within the Production environment must have SC clearance.</p> <p>This requirement is required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail:</p> <ul style="list-style-type: none"> • How, where from and what devices you can use to access the Production area • How you can demonstrate your initial and ongoing compliance with Remote Support users (Production) having SC clearance 	
<p>Introduction</p> <p>We confirm that our solution fully meets the requirement for Remote Production Support. As this requirement is already available for the current service, it will be included for Viable Product Release and the Operational Service Commencement Date.</p> <p>Our proposed solution is a refreshed version of our current platform enhanced with a digital platform supporting much of the new functional requirements. This approach to our solution will not only assure a quick and safe transition but also delivers operational stability and security.</p> <p>Production Environment Access</p> <p><i>How?</i></p> <p>Remote Support for the Production solution, hosted on the IRIS UK Cloud Platform, our UK Government Secure multi-tenanted Cloud platform, will be provided by UK SC Cleared personnel via a dedicated 'UKSecure Support Zone' hosted on the Platform.</p> <p><i>From Where?</i></p> <p>Access to the UKSecure Support Zone is only permitted from Atos IT Services UK Limited UK sites or Atos UK SSL-VPN via end-to-end encrypted TLS 1.2 connection into the UKSecure zone Bastion Hosts. The Bastion Hosts are protected by an isolated Authentication and isolated Two Factor Authentication solution. The entry point is protected via an Intrusion Prevention Service, strict firewall rules and micro-segmentation.</p> <p><i>What Devices?</i></p>	

Support will be provided from Atos UK Windows 10 devices protected by ForeScout, Windows Defender, BitLocker, Azure Information Protection, Restricted User Access and Network Access Control. Access to the Atos UK Network is via SSL-VPN with PKI two-factor authentication.

The Atos Windows 10 Client, IRIS UK Platform including the UKSecure Zone and DWP Zone(s) are subject to an annual CHECK IT Health Check. The IRIS UK Platform is Cyber Essentials Plus Certified (IASME-CEP-006272).

Remote Support Users Security Clearance

All IRIS UK Platform Administrators and Tenant Administrators of the Buyer's Solution hosted on IRIS UK undergo vetting checks to achieve BPSS and Security Clearance (SC).

Tenant Support User Accounts in the UKSecure Support Zone and Customer Zone(s) are only granted to UK engineers with verified Security Clearance via a strict account request and approval process through an IRIS hosted Service Now Catalogue with a full audit trail. Account requests are reviewed by the Atos Client Security Manager who verifies with the Atos UK Security Vetting team the validity of their SC Clearance prior to approval.

The Atos UK Security Vetting team are responsible for all UK employee Security Clearance requirements. The Security Vetting team process several hundred Security Clearance requirements every year for multiple Government customers including BPSS, SC and DV.

A quarterly Security Clearance check of all IRIS Platform, UKSecure and Tenant Administrators, performed by the Atos Client Security Manager captures any personnel with clearance that is nearing expiration. This is reported on at the monthly Security Working Group for the IRIS UK Platform and its tenants. All engineers are prompted to renew security clearance 6 months before expiration by the Atos Security Vetting Team

If for any reason security clearance lapses or is not re-issued before expiration associated user accounts are disabled and deleted.



486 words

4.4m) ITDR	Weighting 0.20% Technical Assistance
Guidance:	
<p>The Buyer will require regular full disaster recovery testing. These should be at minimum run as an annual exercise and results delivered to the Buyer in the form of a Disaster Recovery Report.</p> <p>This requirement is not required for Viable Product Release (See Attachment 6.1)</p> <p>This requirement is required for Operational Service Commencement Date (See Attachment 6.1)</p>	
Question:	
<p>Incorporating the guidance above, your response should detail your approach and frequency of full disaster recovery testing along with a sample outline content of the Disaster Recovery Report.</p>	
<p>We confirm that our solution fully meets the Non-Functional Requirement for ITDR, and that this will be fully established by the Operational Service Commencement Date.</p> <p>Introduction</p> <p>Atos' Disaster Recovery Plans (DRP) delivers capability to recover and resume services to the buyer. Plans and procedures will ensure the continuance of critical business processes and maintain an acceptable level of service during a disaster until full services can resume. The plan will ensure minimal disruption to operations in the event of significant problems and interruptions and ensure organisational stability and an orderly recovery.</p> <p>Disaster Recovery Plan</p> <p>The DRP will cover the worst case of the total loss of a facility including IT equipment and services. It will be written in modules so that in the event of a partial loss, the appropriate plan modules could be used to implement the required recovery actions.</p> <p>The plan will document the procedures to restore each business process based on criticality before the expiration of each maximum acceptable down time.</p> <p>The plan will also define the specific recovery strategies and procedures for meeting these established availability dates in the event of a disaster.</p> <p>A communications strategy will be documented including roles, responsibilities, and key contacts.</p> <p>Atos recognises different levels of disaster recovery tests complexity and the importance of the disaster recovery testing process. All disaster recovery tests serve as verification of the implemented DRP but also as training for the staff involved so that they can easily recall the steps needed in a real disaster.</p> <p>The regular full DR test schedule will be agreed between Atos and the Buyer and will be at minimum run as an annual exercise. The DR test schedule, DR test plan, DR test results and reports are all documented and archived.</p>	



Simplified flowchart of DR testing process

The testing plan will ensure that the recovered area provides the expected service level. However, tests need to be done on each stage of the recovery process to ensure that the systems work together. Atos take full responsibility of the execution of the tests, and the full DR plan and process is a joint collaborative effort.

Atos holds global certificates ISO 9001, 20000, 27001 and ISO22301 certificates are held for specific customers. For all other customers the requirements of ISO22301 are fulfilled because the BCM is part of ISO27001, and ITSCM part of ISO20000. Additionally, internal audits focus on BCM implementation on a regular basis. Atos conducts regular reviews on its own BCM documents and will include the customer in these reviews as far as is practicable.

Sample outline of BCDR Incident and recovery report



Sample outline of
BCDR Incident and r

Date:	00/00/00
Time:	00:00
Name:	
Designation:	

High Level Description of Incident:

In this section you clearly and briefly communicate in brief the incident that has occurred.

For Example:

- Industrial Action
- Pandemic Influenza
- Site Evacuation
- Software Failure
- Loss of Telephony
- Other Incident

Associated Impacts:

In this section you clearly and briefly communicate the specific impacts to your service/function.

For Example

- % Reduction In staff
- Denial of access to premises
- % Reduction in Productivity
- Interdependency e.g. Chennai
- Increased Customer Complaints
- Increased Incoming Calls

Associated Risks:

In this section you clearly and briefly communicate the associated risks, highlighting them as short, medium and long term.

For Example

- Accumulated backlog
- KPI Failures
- Reputational Damage
- Workforce Morale

Mitigations/ Strategy:

In this section you clearly and briefly communicate any implemented or proposed mitigations for the impacts and risks.

For Example:

- Staff redeployment
- Non-critical functions temporarily suspended
- Communications deployed to customers/staff/ client

Resource Requirements:

In this section you clearly and briefly communicate any implemented or proposed mitigations for the impacts and risks.

For Example:

- Number of additional staff required
- Logistics – transport, catering, security, protective equipment, stationary etc.
- Funding, cost codes, emergency budgets



Operational stability
and security

430 words