Crown Commercial Service

RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 2 September 2025 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.
The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website RM6100 Technology Services 3. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

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

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

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

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

1.1.2 the Order Form;

1.1.3 the Call Off Terms; and

1.1.4 Framework Schedule 18 (Tender).

Crown Commercial Service

Section A - General information

Contract Details	
Contract Reference:	Project_9557
Contract Title:	Framework Engineering
Contract Description:	Technical development & support for a suite of shared services that support the Atlas case working system
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	The Anticipated Potential Value and forecasted value of this Call Off Contract is between £54.83m and £87.83m. However, the Services which will be initially commissioned under this Call Off Contract via Statements of Work are based on the Suppliers Charges as set out in Attachment 2 (Charges and Invoicing) which sets the estimated value at as set £54,831,807.64.
Estimated Year 1 Charges:	£16.98m
Commencement Date:	3 November 2025

Buyer details

Buyer organisation name
The Secretary of State for the Home Department

Billing address
2 Marsham Street,
London SW1P 4DF

Buyer representative name
[redacted]

Buyer representative contact details
[redacted]

Buyer Project Reference
itt_79958

Crown Commercial Service

Supplier details

Supplier name
Mastek (UK) Ltd

Supplier address
Part Ground Floor,
North Wing A,
100 Brook Drive,
Green Park, Reading,
RG2 6UJ

Supplier representative name
The name of the Supplier point of contact for this Order
[redacted]

Supplier representative contact details
[redacted]

Order reference number or the Supplier's Catalogue Service Offer Reference Number
A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.
N/A

Guarantor details

Guarantor Company Name
Not applicable.

Guarantor Company Number
Not applicable.

Guarantor Registered Address
Not applicable.

Crown Commercial Service

Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed

1. TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2. TRANSITION & TRANSFORMATION	☐
3. OPERATIONAL SERVICES	
a: End User Services	☐
b: Operational Management	☐
c: Technical Management	☐
d: Application and Data Management	X
5. SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
3	60 (5)

Initial Term Months
36

Extension Period (Optional) Months
12+12

Minimum Notice Period for exercise of Termination Without Cause 90 days
(Calendar days) Insert right (see Clause 35.1.9 of the Call-Off Terms)

Sites for the provision of the Services

The Supplier shall provide the Services from the following Sites:

Crown Commercial Service

Buyer Premises:
2 Ruskin Square,
Dingwall Road,
Croydon,
CR0 2WF

Supplier Premises:
Premises agreed are:
[redacted]

Third Party Premises:
Not Applicable.

Buyer Assets
Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms
For the avoidance of doubt, all Intellectual Property Rights (IPR) belong to the Buyer.

The Buyer will provide access to: (a) the relevant Buyer owned or licensed tools and systems via virtual desktops or Buyer's virtual private network; and (b) POISE devices (i.e., Buyer-issued laptops) when required.
Supplier shall be responsible for provision of laptops to all required resource.
All processing of Buyer Data will be on Buyer systems, except where Buyer Data is required for approved use by the Supplier for incident resolution purposes (subject to the process set out in Attachment 9 (Data Processing) in respect of processing of any personal data), and all processing shall be in accordance with the provisions governing data processing set out in this Contract.

The Supplier shall comply with the geographical restrictions notified to it by Buyer with respect to location of personnel and transfers of Buyer Data, save to the extent that any country has been approved in writing by the Buyer (including on a case-by-case basis and any locations referred to under 'Supplier Premises' and 'Third Party Premises' above).

Buyer will properly maintain its infrastructure and the Buyer Assets (hardware and software) during the term of the Contract.

Supplier is not responsible for and shall have no liability arising out of or relating to, the performance, reliability, availability, or security of any Buyer or third-party system or hardware which is not within the scope of the Services.

Crown Commercial Service

Additional Standards
Guidance Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions).

As per the Appendix A, Section A (Guidance, Standards and Policy References) which includes the Buyer Security Policy standards.

Any updates shall be managed via the Change Control Procedure.

Buyer Security Policy
Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

HMG Security Policy Framework:
https://www.gov.uk/government/publications/security-policy-framework
Cyber Governance Code of Practice:
https://www.gov.uk/government/publications/cyber-governance-code-of-practice
Government Security Classification Policy:
https://www.gov.uk/government/publications/government-security-classifications

Further guidance, standards, and policy can be found in Section A of Appendix A.

Buyer ICT Policy

Home Office Digital Strategy:
https://www.gov.uk/government/publications/home-office-digital-strategy/home-office-digital-strategy
Home Office Technology Strategy:
https://www.gov.uk/government/publications/home-office-technology-strategy/home-office-technology-strategy
Government Service Design Manual:
https://www.gov.uk/service-manual/browse
GDS Service Manual standards and Policies
https://www.gov.uk/service-manual

Further guidance, standards, and policy can be found in Section A of Appendix A.

Insurance
The insurance(s) required will be:

- a minimum insurance period of 6 years following the expiration or ending of this Call-Off Contract
- professional indemnity insurance cover to be held by the Supplier and by any agent, subcontractor or consultant involved in the supply of the this call-off . This professional indemnity insurance cover will have a minimum limit of indemnity of the US$ equivalent of £5,000,000 for each individual claim and in the aggregate
- employers' liability insurance with a minimum limit of £10,000,000 or any higher minimum limit required by Law.

Crown Commercial Service

Buyer Responsibilities
To be mutually agreed between the Parties and set out in each Statement of Work as commissioned under this Call Off Contract.

Goods
Not applicable.

Governance – Option Part A or Part B

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	☐
Part B – Long Form Governance Schedule	☑

The Part selected above shall apply to this Contract.

Change Control Procedure – Option Part A or Part B

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	☑
Part B – Long Form Change Control Schedule	☐

The Part selected above shall apply to this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be N/A; and
- for the purpose of Paragraph 8.2.2, the figure shall be N/A.

Crown Commercial Service

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses (see Annex 3 of Framework Schedule 4)
This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules

Additional Schedules	Tick as applicable
S1: Implementation Plan	☑
S2: Testing Procedures	☑
S3: Security Requirements (either Part A or Part B)	Part A ☑ or Part B ☐
S4: Staff Transfer	☑
S5: Benchmarking	☑
S6: Business Continuity and Disaster Recovery	☑
S7: Continuous Improvement	☑
S8: Guarantee	☐
S9: MOD Terms	☐

Part B – Additional Clauses

Additional Clauses	Tick as applicable
C1: Relevant Convictions	☐
C2: Security Measures	☐
C3: Collaboration Agreement	☐

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses

The following Alternative Clauses will apply:

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

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Crown Commercial Service

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)
To be provided by the Supplier within 20 days of Commencement in line with Schedule S3.

Additional Schedule S4 (Staff Transfer)
Not applicable.

Additional Clause C1 (Relevant Convictions)
Not applicable.

Additional Clause C3 (Collaboration Agreement)
Not applicable.

Crown Commercial Service

Section D - Supplier Response

Commercially Sensitive information
Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Attachment 2 – Charges and Invoicing
Attachment 5 – Key Supplier Personnel and Key Sub-Contractors
Appendix C –Additional Reporting, Value Add and Social Value Bid Commitments

Crown Commercial Service

Section E - Contract Award

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

SIGNATURES

Crown Commercial Service

Attachment 1 – Services Specification

Please see Appendices A, B, and C below. All three Appendices should be read in their entirety as together they form the Services Specification.

See appendix A – Specifications

See appendix B - Level 3 Support Requirements

See appendix C – Additional Reporting, Value Add and Social Value Bid Commitments

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

Not applicable.

Part B – Service Charges

Not applicable.

Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges

The following Charges shall be used and applied to each Statements of Work (SoWs) as commissioned and agreed by the Parties under this Call Off – Contract that will deliver the Services as set out in Attachment 1 (Service Specification) to the Buyer.

Fixed Core Team Rate Card
The Fixed Core Team rates apply to all resources included within SoWs as part of the planned workstream.

[redacted]

Surge Rate Card
This rate card provides rates for unplanned-for surge support not included in regular SoWs and the expected pipeline.

[redacted]

Crown
Commercial
Service

[redacted]

Further information on working pattern and hours can be found within paragraph 5.3 of Appendix A.

Crown Commercial Service

Part D – Risk Register

Risks will be established and described within each Statement of Work as well as subsequently managed and tracked in a contract risk register. They will be reported on regularly in the Balanced Score Card template during the Contract Management Board (as outlined in Attachments 8 – Governance and 10 – Transparency Reports).
The risk register will consider the following items:

Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Owner

Part E – Early Termination Fee(s)

Not Applicable.

Attachment 3 – Outline Implementation Plan

At least 20 days prior to commencement, the Supplier shall provide a draft implementation plan (See Annex S1 of Framework Schedule 4 – Annex 3) for review by the Buyer.

The mobilisation plan shall maintain current capacity, but focus on reducing the offshoring available under the previous contract and ensuring all governance, project road mapping, processes & reporting are in line with the requirements and specifications outlined in Attachment 2. In particular, the Supplier will:

- Propose targets for KPIs without service credits for the Buyer to review
- Prepare to meet new management information requirements
- Review their existing ways of working and collaboration with the Buyer and prepare any changes required
- Assess new governance arrangements and prepared any changes as required
- Assess the Key Stakeholders and changes required
- Prepare to provide agreed performance metrics
- Review and plan to deliver all obligations documented through the procurement process, including but not limited to the obligations delineated in Appendices A, B and C
- Complete a risk review and propose any salient risks for the Buyer's review, to be included in the risk register
- Develop a plan to move to a new team structure, in particular any onshoring or nearshoring requirements
- Support the Buyer in any forecast requests as part of contract budget activity

The Supplier has committed to leading services in Month 1 post-contract award, working with the Framework Engineering (FE) Product Owner and Delivery Manager to allocate core and surge teams based on capacity and backlog. These teams will deliver against the FE backlog and milestones throughout the Outline Implementation Plan and beyond.
Additionally, in the initial 3 months, the Supplier will invest approximately 80 person-days as a value-add initiative to assess the wider portfolio and recommend products for technical debt prevention and continuous capability management to improve MPTP release quality and cadence.

Attachment 4 – Service Levels and Service Credits

Service Levels and Service Credits

The supplier must adhere to the following Key Performance Indicators (KPIs) as derived from Appendix A - Specifications:

Theme	KPI and rationale	Measurement and frequency	Targets
Code Quality	Maintain & Improve SonarQube Code coverage at AutoSIT: Ensures adherence to coding best practice, maintains code quality, and detects errors early for sustainable, reliable production.	SonarQube code coverage, Monthly	See the table below for the Service Credits applied
Testing	Functional Code failures in PRP 1 & 4 environments: Aims to minimise deployment failures in live environments (PRP1, PRP4). Pre-production code is highly integrated, and functional failures can slow down overall delivery and block the production pipeline.	P1/P2 failures in PRP1 and PRP4 environments per sprint across sprint teams of FE, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12 in Appendix A - Specifications
Lead Time to Change[1]	Lead time to change measures the average time it takes for a code change to be deployed to production: A shorter lead time indicates a faster and more efficient delivery process, enabling faster time to market and quicker response to customer needs.	Total lead time for all deployed changes / Number of deployed changes, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12 in Appendix A – Specifications
Cycle Time (dev)	Time it takes for a work item to get from the moment work starts (starting with 'In progress' status to when it is delivered 'Done' or 'Live'). *Tracking cycle time to restore pre transition, we can identify bottlenecks, optimise workflows, and improve overall productivity*.	Total cycle time for all completed items / no of completed items, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12 in Appendix A – Specifications
Deployment Frequency[1]	Frequent deployments to Production: Crucial for continuous delivery, ensuring frequent	Deployments to Production per sprint across sprint	To be determined during onboarding in accordance with paragraph 6.6.12 in

	deployments that enhance agility, deliver quicker value to users and stakeholders, and provide more opportunities for feedback.	teams of FE, Monthly	Appendix A – Specifications
Platform Stability in Production (failed change) [1]	Production Outages P1 or P2 because of FE code changes deployed in the last 5 working days (identified by through RCA): *Aims to minimise production outages to enhance case worker productivity and product perception.*	Number of outages by quarter across sprint teams of FE, Quarterly	See the table below for the Service Credits applied
Service Availability	The percentage of time a service is operational and available to users: It assesses the reliability and uptime of the service, ensuring it meets the (MBTP) (NFR).	Total uptime / (total uptime + total downtime), Monthly	99.9% availability, during core hours, excluding outages due to releases or environment unavailability (as outlined in Appendix B – Level 3 Support Requirements)
L3 Response Time	The efficiency and speed of responding within the team for P1, P2, P3, and P4: Tracking time to respond, we can identify bottlenecks, optimise workflows, and improve overall productivity	% of tickets responded to as per the SLAs in the Level 3 Requirements Document, from ticket assigned to FE to ticket closed, Monthly	<30 minutes for a P1 incident <30 minutes for a P2 incident <12 working hours/1.5 day for a P3 incident <24 working hours/3 days for a P4 incident (For further details, see Appendix B- Level 3 Support Requirements)
L3 Restoration Time[1]	The efficiency and speed of restoring services within the team for P1, P2, P3, and P4: Tracking time to restore, we can identify bottlenecks, optimise workflows, and improve overall productivity	% of tickets resolved as per the SLAs in the Level 3 Requirements Document, from ticket assigned to FE to ticket closed, Monthly	<4 hours for a P1 incident <8 hours for a P2 incident <24 working hours/3 days for a P3 incident <40 working hours/5 days for a P4 incident (For further details, see Appendix B-

			Level 3 Support Requirements)
Social Value 1	Tackling economic inequality: Create employment and training opportunities particularly for those who face barriers to employment and/or who are in deprived areas, and for people in industries with known skills shortages or in high growth sectors	Number of full-time equivalent (FTE) employment opportunities created under the contract, by UK region, Yearly	To be determined during onboarding in accordance with paragraph 6.6.12 in Appendix A – Specifications
Social Value 2	Equal opportunity: Increase representation of disabled people and tackling inequality in the contract workforce	Total percentage of full-time equivalent (FTE) disabled people employed under the contract, as a proportion of the total FTE contract workforce, by UK region, Yearly	To be determined during onboarding in accordance with paragraph 6.6.12 in Appendix A - Specifications

[1] These are KPIs that map back to the DORA metrics.

[redacted]

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
[redacted]	[redacted]	[redacted]

Part B – Key Sub-Contractors

Not applicable.

Attachment 6 – Software

All Intellectual Property Rights (IPR) belong to the Buyer.

Further information on IPR, and on the licensing of any Software below, is in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software

Not Applicable

Part B – Third Party Software

Not Applicable

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the schedule will be replaced by Definitive Joint Schedule 7 (Financial Difficulties) which can be found in the Additional Annexes (which are attached separately).

Attachment 8 – Governance

Part A – Short Form Governance

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Operational Board – Monthly Balanced Scorecard Meeting	
Buyer Members for the Operational Board	Not applicable.
Supplier Members for the Operational Board	Not applicable.
Frequency of the Operational Board	Not applicable.
Location of the Operational Board	Not applicable.

Part B – Long Form Governance

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

Contract Management Board (Service Management, Change Management, and Risk Management to be covered within)	
Buyer Members of Service Management Board (include details of chairperson)	Commercial Lead Lead Product Manager Delivery Manager
Supplier Members of Service Management Board	Contract Manager
Start Date for Service Management Board meetings	From date of contract signature.
Frequency of Service Management Board meetings	Monthly
Location of Service Management Board meetings	Online.

Operational Management (Technical) Board	
Buyer Members of Technical Board (include details of chairperson)	Delivery Manager
Supplier Members of Technical Board	Delivery Manager
Start Date for Technical Board meetings	From date of contract signature.
Frequency of Technical Board meetings	Weekly
Location of Technical Board meetings	Online or at the agreed premises outlined in Part B, to be agreed between attendees.

The supplier must also attend programme delivery boards, steering groups and change boards if necessary to explain impact assessments, review operational delivery, and address risks, mitigations and escalations.

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [redacted]
1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [redacted].
1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.
1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	The Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data: • Personal data required for Casework Application Processing will be transmitted through Atlas Interfaces Software; and Daily Operational Dashboards that the Supplier team will develop. Please note that Processor will not be sourcing this data nor will the Processor manipulate this data. The developed software will be hosted on Controller's infrastructure and any data manipulation will be done by the Controller's personnel through application user interfaces. Access to such data will be restricted to a limited number of SC cleared Supplier Staff. The Supplier is Controller and the Authority is Processor The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Authority is the Processor in accordance with Clause 34.2 to 34.15 of the following Personal Data: • Supplier Staff Details The Parties are Independent Controllers of Personal Data The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel, Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Authority's duties under this Contract.
Duration of the processing	The processing will start when the services delivered by the Supplier under this contract are commenced on 3 November 2025 and processing will cease when the supplier exits.

Nature and purposes of the processing	The purpose of Processing is to enable the Authority's staff to progress and decide on outcomes on immigration services enabled by the Suppliers software.
Type of Personal Data	This may include but is not limited to: Personal data including name, nationality, immigration history, unique IDs, present and past addresses, information relating to passports and / or other identity documents, date of birth, reference numbers held by the Home Office and / or other agencies and government departments, together with similar details for family members, emails and phone numbers. Special category data including person alerts that relate to health. Criminal offence data including criminal record, detention type and
Categories of Data Subject	• Any persons with an involvement in relation to immigration case-working. • Supplier staff who provide casework service delivery and support and Authority's staff who process immigration caseworking.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	All data is stored in AWS Cloud Instances owned by the authority and retained in line with the Authority's Security and Data Retention Policy. Any data no longer required for processing will be automatically purged from the system based on agreed rules for data persistence (which the Controller will manage given the processing is on Controller's platform).

Attachment 10 – Transparency Reports

The Supplier shall report on the contract performance monthly in the Contract Management Board (as outlined in Attachment 8 – Governance), using a Balanced Score Card template provided by the Buyer and included in the Additional Annexes.

Appendices A, B & C – Services Specifications

Appendix A – Specifications

2. DIGITAL, DATA AND TECHNOLOGY

2.1 Digital, Data and Technology (DDaT) provides technology delivery and live operational support for the Home Office (HO) IT estate. DDaT's mission is to put users at the heart of everything, work collaboratively to design, deliver and continuously improve the digital products and services that enable a safe, fair and prosperous UK.

2.2 DDaT Objectives are as follows:

a) Build and sustain a brilliant DDaT capability where everyone realises their full potential.
b) Create a diverse and inclusive environment that promotes wellbeing.
c) Deliver digital services that automate processes to drive transformation.
d) Be a trusted partner and foster innovation.
e) Embed a product way of working that delivers value faster.
f) Design, build and maintain secure and resilient products and services.
g) Passionately drive an improved experience for our users.
h) Modernise and converge our technology, reducing technical debt and legacy.
i) Exploit our data assets to enable better insights and outcomes.
j) Optimise our cost base and deliver best value for money.

2.3 DDAT activity can be categorised in three areas, all of which are described further in section 3:

a) Run – Level 3 Support (see 4.7) – effective and efficient incident management, problem management, change and continual improvement.
b) Sustain – patching, upgrades, maintenance and addressing/managing technical debt.
c) Change – significant technical development and delivery for major programmes and organisational objectives including path to live activities.

2.4 **Migration and Borders Technology Portfolio**

2.4.1 The Migration and Borders Technology Portfolio (MBTP) is a part of DDaT. MBTP provides technology delivery and live operational support for Migration, Asylum and Border control. MBTP uses Agile delivery methods to deliver outcomes, under a shared governance structure which ensures alignment with wider organisational objectives and priorities. It is a dynamic environment with changing priorities so teams must be able to adopt a flexible approach to planning, delivery and support.

2.4.2 The Portfolio is responsible for the following major programmes:

[redacted]

2.4.2.2 Future Borders Immigration System (FBIS) – see 2.5

2.4.2.3 Digital Services at the Border (DSAB) [redacted]

2.4.2.4 Asylum and Protection Transformation [redacted]

[redacted]

2.5 **Future Borders and Immigration System**

2.5.1 Established to lead on the design and delivery of a new immigration system following the UK's exit from the European Union – FBIS builds upon technology developed as part of the EU Settlement Scheme.

2.5.2 Tranche 1 consisted of extending sponsorship to EEA citizens, work and study routes (sponsorship transformation), new routes and extending existing routes for EEA citizens and transforming the skilled worker route.

2.5.3 FBIS Simplify consists of sponsorship transformation and new routes (inc. development of a Graduate route).

2.5.4 FBIS Enable consists of Identify (capturing once, as early as possible), Status (giving people the ability to prove their rights), Customer (improving our customer service offer) and Caseworking (including achieving efficiencies throughout operations / automating tasks).

[redacted]

2.6 **Atlas Overview**

Atlas is the business-critical system used by caseworkers to manage the processing of visa and asylum applications. It also provides operational functionality for Border Force and Immigration Enforcement. The system has a requirement to be "available" 24 hours a day, 7 days a week, with updates and enhancements continually delivered to enhance its functionality and capabilities.

2.6.1 Atlas currently supports circa 30,000 users globally, anticipating 47 million applications per year:

- Electronic Travel Authorisation (ETA) applications making up 35-40 million cases
- Out of Country cases contributing 5 million cases
- In Country caseworking contributing 2-3 million cases.

2.6.2 The vision for Atlas is development and growth following a product-first approach, rather than driven by a series of programmes and projects. It will continue to be developed for future expansion to support strategic departmental initiatives. Currently the future ways of working are being developed between MBTP and a business led Casework Capability team.

2.6.3 Atlas is a containerised Open-source Java microservice application deployed into AWS, which orchestrates workflow following BPM (Business Process Management) processes, triggered by events. Using agile release trains which groups microservices for release.

2.6.4 Other technologies used include:

2.6.5 The Atlas design includes ‘caseworking verticals’ supporting business fulfilment processes (see 3.2.4), which reside in a mono repository. Each ‘vertical’ is built in Java with a user interface and support the business process management (BPM). Tasks are rendered and taken through the process workflow. Current levels of coupling mean code deployments are merged which impacts delivery throughput.

2.6.6 Through the duration of the contract all Suppliers will need to collaborate on initiatives to decouple the current configuration and take opportunities to extend independent activities and code deployments.

2.6.7 Each team developing on Atlas has some DevOps capability and is responsible for deploying, maintaining and managing their own databases e.g. PostgreSQL RDS.

2.6.8 Code is stored in shared libraries and configured via internal tooling, ownership of libraries has been agreed and development teams collaborate on updates.

2.6.9 Atlas serves and manages a set of integrations including:

- The above are the main integrations however there will be other internal connections and downstream consumers that will be included as part of Knowledge Transfer.

3. TECHNICAL LANDSCAPE

[redacted]

[redacted]

[redacted]

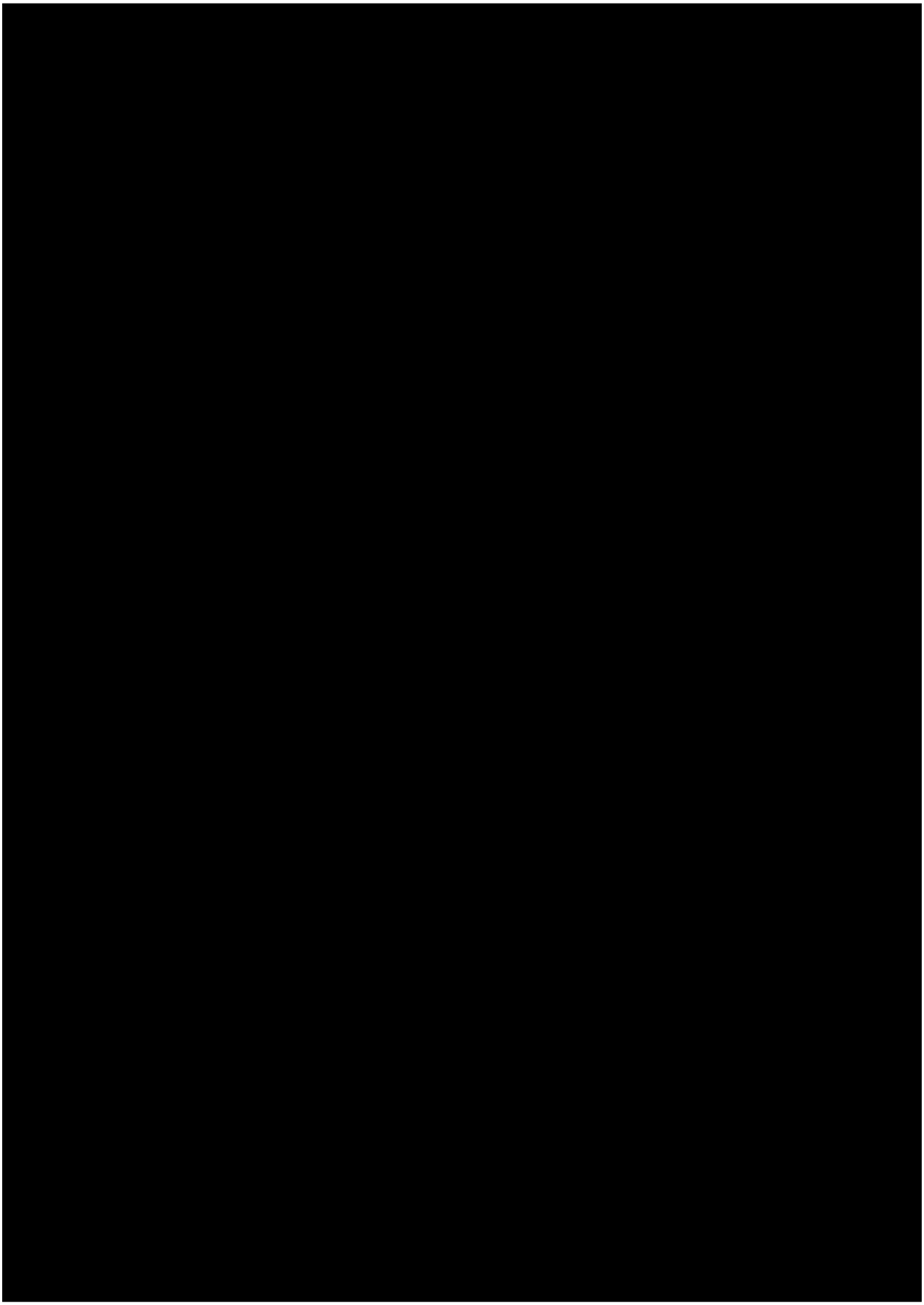
[redacted]

[redacted]

[redacted]

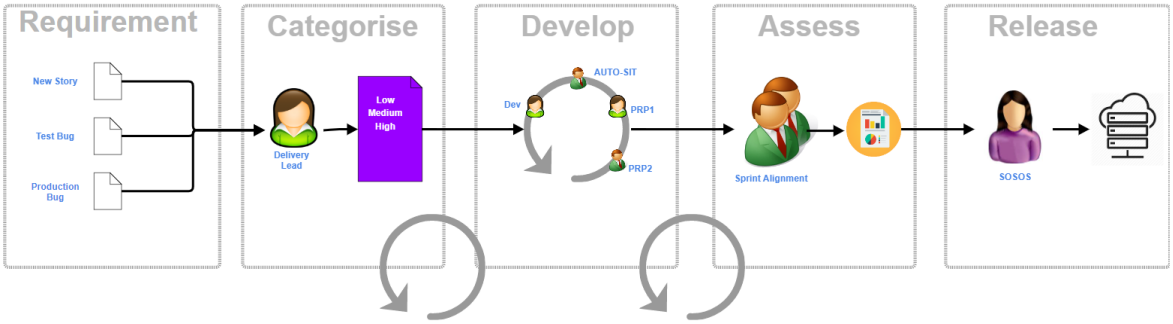
[redacted]

[redacted]



3.3 **Atlas Path to Live**

3.3.1 Below is a high-level overview of the typical Atlas path into the Production (live) environment. This is common across all Atlas caseworking delivery teams.



3.3.2 Requirement(s)/change request(s) can be raised by a Product Owner, MBTP Team, as a result of a discovery from the Business Architecture & Analysis Team, FE requests, or from other workstreams and programmes. They could be for new components and services, new cross-cutting functionalities or functional and non-functional improvements to existing products and services. FE will identify improvements to services and work to maintain:

(a) Performance

(b) Availability

(c) Resilience

3.3.3 The request is Impact Assessed (IA) so effort, cost and delivery date can be provided in line with the team's roadmap.

3.3.4 The IA is then taken through the appropriate governance process for build approval. This can consist of a number of gates depending on the size, complexity and cost.

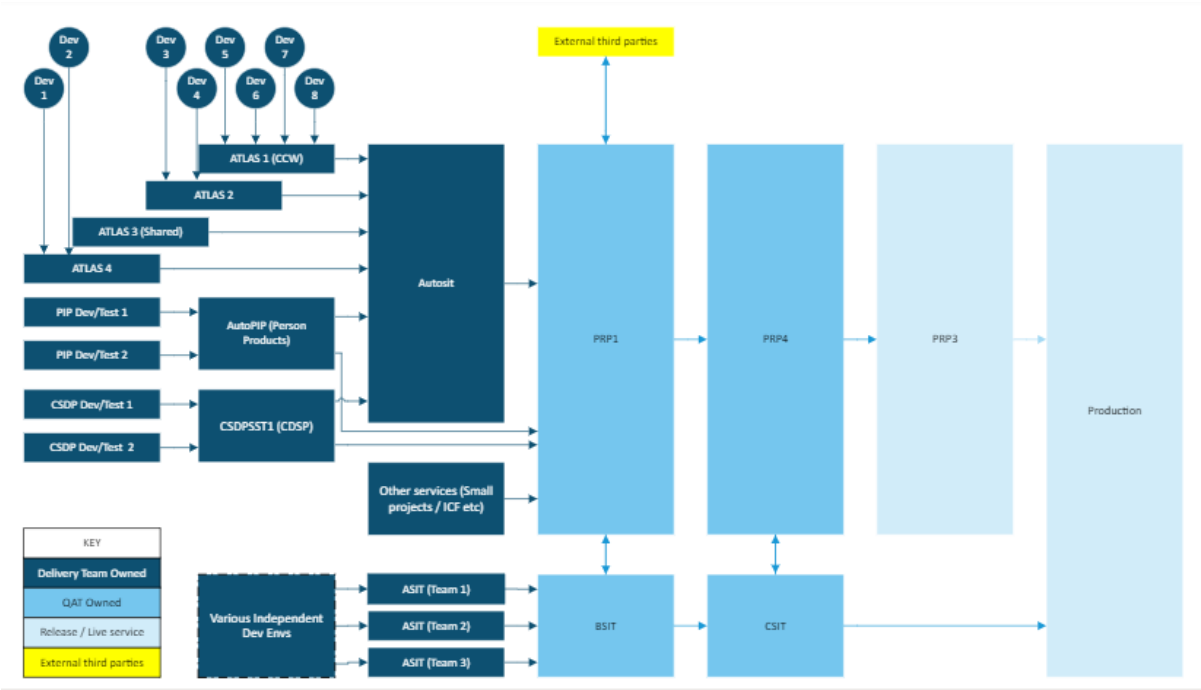
3.3.5 Once approved, the change or new deliverable is scheduled into the team's roadmap and, if cross-cutting, other team's roadmaps for development and test, ensuring dependencies are agreed with other teams.

3.3.6 Once development is complete, the team manages the change through one of two pipelines - the Atlas Release Management process or the Strategic Route to Live (see 3.5). This consists of testing in a number of lower environments and environments specifically focused on integration, OAT (including accessibility testing) and performance testing to assure it is ready for safe release into the Production environment i.e. to go live. The DDaT Change and Release Management team oversee this process. The diagram below provides an overview of the complexity of the Atlas Test and Release Environments (see 3.4.1).

3.3.7 If the deliverable is a new component or service (more frequent for the FE Team due to the nature of the shared components it delivers), it may require an IT Health check/penetration testing. The FE team would be responsible for remediating any vulnerabilities identified in line with cyber security policies and procedures.

3.4 **Atlas Test and Release Environments**

3.4.1 The below chart provides an illustration of the test and release environments:



3.5 **Decoupling and Delivery Pipelines**

3.5.1 The vision for MBTP is to, wherever possible, have independently deployable services on the same pipeline. Strategic Route is Live is the initiative responsible for implementing the solution to resolve delivery and throughput changes for the portfolio by:

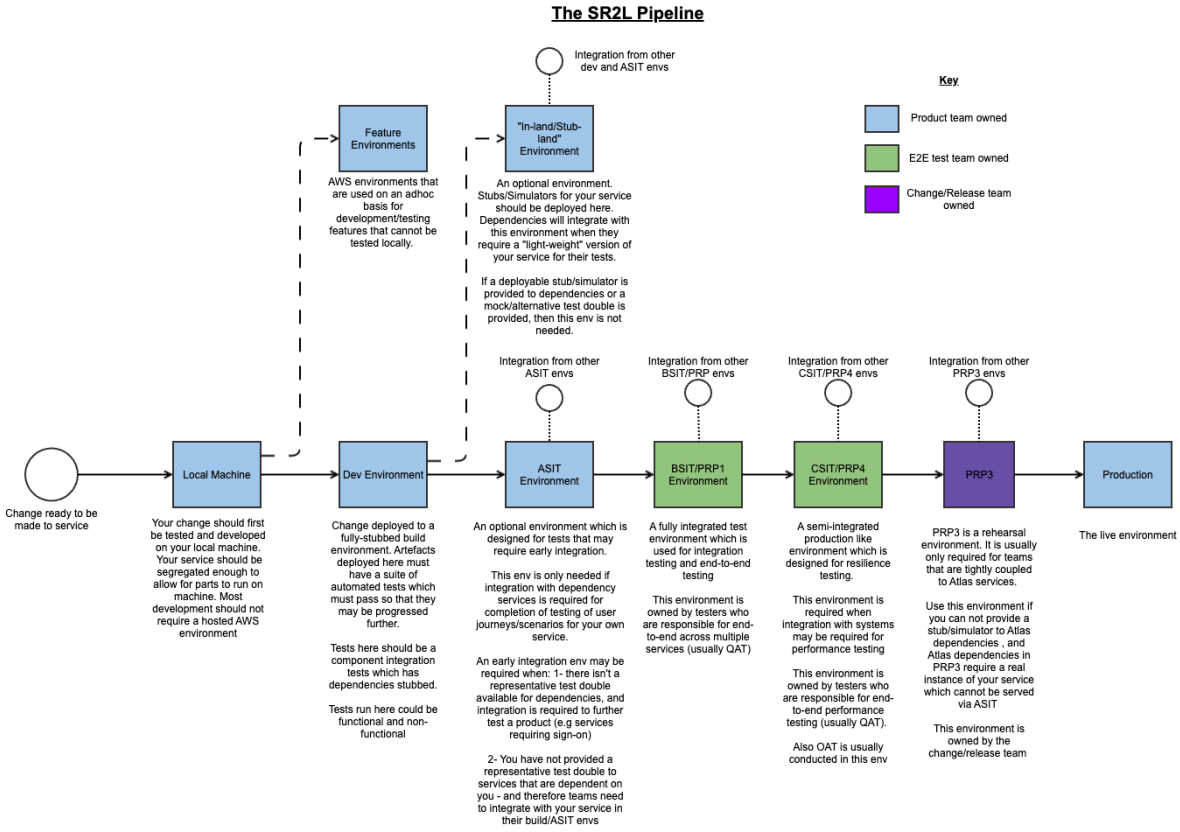
- Changing the pattern to deliver quicker through smaller, more frequent and independent releases, and
- Using standardised tools so that second line assurance is done more efficiently.

This will deliver the following benefits:

- Improved delivery speed through better engineering practices and architectures,
- Reduction in defects in outcomes through use of standard tooling, and
- Improved planning achieved through data-driven processes.

FE is at the forefront of this initiative as an early adopter and the Supplier is expected to continue to provide skills and expertise to support this work which, in turn, aligns with the MBTP software delivery strategy.

3.5.2 The below chart provides an overview of the Strategic Route to Live (SR2L) process:



3.6 **Service Transition**

3.6.1 The Supplier is expected to transition elements of the delivery to BAU live services teams. They will need to engage with DDaT Service Design and Transition and comply with the DDaT Service Design & Transition Governance and Process. In addition, some new or updated FE components and services will also need to be managed through the central DDaT Service Transition process i.e. transition into private beta, then to public beta through to Early Live Support, during which time knowledge transfer and handover takes place to the central HO Level 2 Team and the FE Level 3 team.

The FE Development Team are responsible for:

- engaging and working with the Service Transition Manager to identify the appropriate transition approach
- carrying out transition activities, completing the required documentation and seeking approvals in a timely manner e.g. from security, operational acceptance testing, support teams etc.
- meeting the required standards
- liaising with the Level 2 and Level 3 support teams to achieve acceptance.
- managing and updating the suite of Service Transition JIRA tickets which track sign off through the transition stages.

4. SUPPLIER REQUIREMENTS

4.1 **Requirement Overview**

MBTP requires a Supplier to provide highly skilled specialist technical resources i.e. Technical Architects, a broad range of software engineering skills, test resources, business analysts and delivery professionals with a management wrapper, to deliver the required service to build and support our digital caseworking system. The tools developed by the Supplier are utilised by caseworking.

4.1.1 The Supplier shall support agile development methodologies and will deliver work according to an agreed product roadmap. The roadmap captures deliverables from a number of areas e.g. programmes delivering portfolio objectives, existing backlog, technical debt, other MBTP teams, wider organisational objectives and Ministerial priorities and operational demand.

4.1.2 The Supplier will look to support and run various aspects of the governance process, as well as suggesting any ideas for improving the overall governance or workflow to best optimise delivery whilst remaining economically prudent.

4.1.3 We would look for appropriate engagement from the Supplier in all stages of delivery, from entry and discovery to impact assessment and delivery to live. We would encourage a practical approach in engaging with Business Analysts, Product Managers, Lead Delivery Managers and Technical & Security Architects to ensure requirements are clear, estimates are accurate and overall delivery predictable.

4.1.4 The Supplier will work with other development and support teams, collaboratively, co-operatively and in partnership to ensure the integrity of the overarching Digital Services capability DDaT provides to its customers, end users and partners. Specifically:

- BAU Live Services operational teams (such as MBTP support teams)
- Build teams in other product families
- Improvement teams in other product families
- Central MBTP functions e.g. Business Architecture & Analysis, Solution Design, Technical Architects/Chief Engineers, Cyber Security, Service Transition and User Centric Design.
- MBTP support teams
- Government Partner teams

4.1.5 The objective of the new Contract Provision is to ensure that the Supplier:

- Provides Digital Services teams for the scope as set out within this document.
- Delivers a flexible, responsive yet predictable service provision, supporting the delivery of the FE roadmap and specifically for FE shared services (see 4.2).
- Creates collaborations and partnerships where applicable, that ensure that delivery teams are supportable with agreed repeatable processes in place.
- Aligns with exiting delivery strategies but devises improvements and enhancements, based on analytics to maintain value for costs and quality of service.
- Supports the live services and Operational Support teams.
- Improves the products in order to enhance the live services.

- Builds new features to maintain the relevance of the live services in a digital landscape.
- Works in partnership with all stakeholders in DDaT and its partners in an atmosphere of openness and transparency.
- Uses performance metrics and reporting to continuously improve ways of working.

4.2 **Delivery**

4.2.1 Delivery Scope and Objectives:

The following broad set of requirements outline the key areas required across all services in scope:

1. Technical and delivery leadership that is aligned with and committed to supporting the Home Office in delivering our strategic vision and objectives. We want a Supplier that will own these objectives alongside Home Office teams and take responsibility for realising the vision.
2. **Software developments teams for each of the services in scope**. The teams will deliver work according to a prioritised product roadmap working with MBTP product owners, architecture, UCD and delivery teams. Work will be a mix of continuous improvement, technical debt and new functionality and will often be cross cutting and complex.
3. **A Supplier with a proven track record of delivery in complex environments**. Managing the challenges of legacy systems, legacy data and transitional architecture in a cross-cutting multi supplier environment.

4. **Third line support for services (24x7 as required)**. See section 4.7 for details on support requirements.

4.2.2 The Supplier will be required to ensure knowledge transfer to Home Office civil servant staff who may join the team to work alongside the Supplier. This will be an ongoing process, and not confined to the Contract exit provisions.

4.2.3 The Supplier shall:

- work with the FE Product Manager and Delivery Manager to develop and deliver the FE Product Roadmap supporting portfolio objectives and strategy.
- Deliver the product roadmap using a range of structured programme and project management methodologies, including Agile at scale and pace.
- Plan with capacity for the team to deal with high priority ad hoc issues.
- Utilise HO project delivery lifecycle methodology and toolset where required.

4.2.4 Plan in accordance with Portfolio Programme Increments process. PI (Programme Increment) Planning is a cadence-based event that happens every eight weeks to ensure teams are working towards clear objectives and priorities set by the MBTP. Within the session, there is an agenda for the day compiled of roughly 40 teams who present their plans for the next PI (the next eight weeks) and dependent teams assure the plans presented. The teams present a ‘one pager’ which is the template they present their plans from. Often teams go through an onboarding process and training before being added to the PI agenda. The supplier will be expected to manage the one pager production and present in the PI Planning meetings.

4.2.5 Collaborate with Portfolio Business Engagement leads/Business Architects and Analysts to complete early analysis of proposed improvements to develop the initial business requirements.

4.2.6 Monitor and develop metrics to demonstrate team progress/ performance that will inform the project plans so outcomes/ milestones will be more predictable.

4.2.7 Develop team productivity through reviewing team metrics to identify improvements.

4.2.8 Proactive monitoring of dependencies, interdependencies within programmes or between related projects, risks, and issues – with timely escalations when appropriate.

4.2.9 The Supplier is expected to transition elements of the delivery to BAU live services teams. They will need to engage with DDaT Service Design and Transition and comply with the DDaT Service Design & Transition Governance and Process.

4.2.10 The Supplier will be expected to train Civil Servants in line with any Service offering of training; this should include day to day tasks, tooling, and integrations.

4.2.11 The Supplier is expected to provide highly skilled, experienced resources and capabilities i.e.:

- Technical, architectural, delivery and test resources to maintain, develop and enhance Atlas.
- A dedicated, and where required 24x7, live support (level 3) team to keep Atlas operational, recover from live service incidents and to enable it to scale in line with its significantly increasing user base.
- Experience in managing, delivering and supporting complex solutions in large agile product portfolios.
- Experience in multi-supplier ecosystems as integrator and/or partner supplier.
- Agility to quickly respond to changes required in development team capacity (increasing or decreasing resources).
- Comprehensive skills in line with the current technology stack.
- Experience of managing and supporting Government applications and services, with appropriate Government compliant onshore resources and facilities; any offshoring (see Section A) would need to comply with strict Government security policy.
- Track record of innovation and leadership to drive continuous improvement.
- Ability to drive the convergence and the use of shared technology and resource.
- Commitment to use and integrate to client-side management tools for tracking and managing incidents, service requests, changes, and problems.
- Ability to support (at least) twice weekly releases (on Atlas Release Assess pipeline), comprising of multiple development changes across services – for context, there have been 2500+ code releases across Atlas each year since 2021.

4.2.12 The broad responsibilities that we expect the Supplier to manage and to apply best practises and expertise to:

- Ensure the Atlas Shared Services:
  - remain resilient, performant, scalable and secure
  - remain available,
  - develop in line with requirements generated from portfolio priorities/overseas transformation & through consolidation of Portfolios, and
  - align with EBSA (the platform Atlas is hosted on) cost and security standards.
- Propose new initiatives to improve platform/service and reduce cost.

- Enforce code standards within portfolio – for consistency and ease of maintenance (see Section A).
- Collaborate with Atlas architects and portfolio Architects on best practices.
- ensure designs are submitted to design assurance and maintain compliance to Technical Design Authority standards (see Section A).
- Ensure compliance with Government and HO standards and policies (as outlined in Section A)

4.2.13 DDaT expects all stakeholders, partners and suppliers to work collaboratively, transparently and in partnership to successfully achieve its outcomes.

4.2.14 As part of this contract, and where practicable, the Supplier is obliged to work alongside civil servant team members to increase knowledge and experience within the Civil Service.

4.3 **Architectural Support**

4.3.1 Supplier Technical Leads will work with the Portfolio Technical Architecture/ Security Supplier & EBSA team to maintain and develop the Atlas Shared Services, aligning with Portfolio and HO DDaT strategies and policies. Consideration will need to be given to the Government's digital and technology transformation agenda & outcomes aligned with Government Digital Service Standards.

4.3.2 The Supplier shall:

- Maintain current baseline architecture for the Atlas Shared Services.
- Develop the target architecture for Atlas Shared Services in alignment with business drivers and ensure adherence to portfolio technical strategy and standards.
- Document the architecture to agreed standards.
- Evidence the appropriate sign-off of designs at portfolio TDA and relevant design authorities.
- Implement designs as agreed at portfolio TDA - if deviation in specification is required, raise to portfolio TDA for approval and report deviation to the HO Product and Delivery Managers via the monthly reports (see 6.6).
- Ensure the shared service architecture aligns with the MBTP strategies and standards while meeting the business objectives and alignment with delivery.
- Ensuring key cross-cutting concerns are addressed in the architecture (reliability, security, cost effectiveness, supportability, performance).
- Analyse the gaps between the baseline and target architecture for the Atlas Shared Services and identify candidate items for an architecture roadmap.
- Develop, implement and maintain an architecture roadmap for the Atlas Shared Services with the supporting implementation and migration plan, based upon an agile delivery runway for programmes and projects and the gap analysis between current and target states.
- Determine an appropriate incremental approach to transition that will deliver continuous business value.
- Develop, implement and maintain architecture principles and constraints to guide development and engineering, while maintaining compliance with MBTP architecture principles.
- Identify where there will be potential IT health checks required and ensure early engagement with the security team.
- Ensure architecture outcomes and artefacts are created using industry standards notation, while maintaining compliance with MBTP architecture principles.
- Provide delivery governance and management to align delivery with Portfolio requirements.
- Provide quarterly periodic updates to Portfolio Architecture leads.
- Maintain a technical debt register correctly categorised and scored.

- Attend and provide input into weekly Chief Engineers meetings.

4.4 **Development, Engineering and Testing**

4.4.1 We often have several competing requirements to deliver for transformation milestones, while also needing to ensure they are engineered in a way that ensures configurability, the ability to accommodate changes in priorities, and ultimately stability in Production and the minimisation of issues in Production.

4.4.2 Supplier Technical Leads will work with the Portfolio Technical Architecture/ Security Supplier & EBSA team to maintain and develop FE components and shared services, aligning with Portfolio and HO DDaT strategies and policies. Consideration will need to be given to the Government's digital and technology transformation agenda & outcomes aligned with Government Digital Service Standards.

4.4.3 To ensure service stability, technical debt must be identified and fixed in a measurable and pro-active manner.

4.4.4 We require the Supplier to be able to implement a process to define, measure and interpret metrics from FE components and shared services and be able to recommend improvements that can then be measured in production, both in terms of reducing incidents and improving reporting, alerting, reliability and availability of the product by the end of the transition period.

4.4.5 This will help drive the transparency of product engineering roadmaps and ensure a strong value linking improvements in the backlog to product value enabling a data driven approach to demonstrate value in fixing technical debt.

4.4.6 The Supplier will deliver high standard quality code to develop and implement new features/enhance existing features using AWS cloud native microservices. They will evolve and transform FE components and shared services to deliver high performance, resilience, stability, and minimal downtime.

4.4.7 The Supplier will:

1. Understand clients' applications requirements and deliver cost optimised solutions.
2. Consider accessibility requirements (see Section A)
3. Work with other teams to set specifications for new applications.
4. Write high-quality source code to program complete applications within deadlines and use Sonarqube to show coverage of tests
5. Progress the deployment through various environments/ phases by way of release trains.
6. Troubleshoot applications, find bugs and offer timely solutions.
7. Test existing applications, identify deficiencies and offer solutions.
8. Prepare and document applications operating instructions, guides for support teams and users so that it can be referred later when needed.
9. Monitor and deliver any software updates to third party components or libraries required due to:
    - closing of support window
    - deprecation or removal of support
    - new CVEs or other identified security vulnerabilities
    - Version is not more than two major versions behind the latest release.
    - Identify and deliver opportunities for consolidation/rationalisation/ optimisation of components or libraries to reduce maintenance/ operational costs going forward.
    - Deliver changes necessary due to a change in the legal environment, such as DPA.

4.5 **Dev-Ops**

4.5.1 The Supplier shall:

- Monitor Atlas Shared Services performance and make necessary changes to meet & exceed Portfolio Non-Functional Requirements (NFRs)
- Monitor Atlas Shared Services and ensure it can scale in line with projected user volumes driven by future projects and initiatives
- Identify and address single points of failure across the platform
- Identify and address platform resilience concerns
- Review Atlas Shared Services monitoring and reporting capability – deliver improvements in monitoring to pre-empt and issue and improved logging to reduce time for support team to complete investigation
- Support initiatives to reduce deployment downtime
- Deliver new functional changes requested by the business that require changes to core capability
- Identify common logic in workstreams to be moved into new common components.
- Meet the definition of done including aligning with the HO DDaT test strategy.
- Provide and manage a fully automated CI pipeline for deploying and managing Atlas Shared Services, utilising CI technologies (such as Jenkins, Docker and Kubernetes, MBTP pipelines) Lead on innovation engineering in the agile delivery lifecycle.
- Lead on performance engineering and being accountable for the performance of Atlas Shared Services.
- Ensure continued development, implementation and maintenance of a robust, scalable security solution in conjunction with the HO DDaT security architecture team.
- Provide a Dev Ops capability for Jenkins environments and using Jenkins in the Atlas Release Assess pipeline – support/ improvements/ optimisation initiatives/ maintenance.
- Build and deploy bespoke monitoring for Atlas Shared Services.
- Provide documentation associated with the delivery.
- The Supplier is expected to support and maintain performance and availability of the Atlas Shared Services to ensure case work system is available to the Business Teams. In the event of Live Service incidents, they are expected to collaborate with Live Service teams to resume services and support the Level 3 team with an incident if needed, following standard Live Service processes where required.

4.6 **Testing:**

4.6.1 As part of the Test Plan (see annex S2 of Framework Schedule 4 – Annex 3) the Supplier will incorporate all of the below at a minimum:

- Links to the Portfolio Test Team and compliance with HO Test Framework and Portfolio Test Strategy.

- Unit Testing
- Component Integration Testing
- Functional / System Testing, including regression testing – automated and manual/ exploratory
- Contract Based Testing (CBT) & early integration testing
- Accessibility aligned with Portfolio Guidance and Web Content Accessibility Guidelines (WCAG) including ongoing reviews and revisions
- Early performance / benchmarking
- Testing to ensure Non-Functional Requirements and overall Operational Resilience, and Disaster Recovery are met including the following deliverables (but not exclusive):

  - Recovery Processes
  - Backup Polices
  - Application Logging
  - Log Aggregation Specification
  - Audit Event Logging (SIEM)
  - Monitoring & Alerting Specification
  - Operational Procedures / Work Instructions
  - Archive/Purge/Housekeeping Specification
  - Error codes and error recovery Work Instructions
  - Operational Service Dashboards
  - Support & Licensing
  - Role Based Access Control (RBAC)
  - Network and Connectivity Testing
  - Infrastructure Build Testing
  - Demonstration of ongoing delivery quality / product assurance with compliance to standards and processes, such as Cyber Security Strategy (including Secure by Design), GDPR, SRE and SEGAS
    - Security considerations including routine running of scanning such as Trivvy, Clare, Burpesuite with remedial actions to address and identified vulnerabilities
    - Routine running of code coverage tools such as Sonarqube with actions to address quality issues
    - Adoption of “shift left” approach to testing and test accountabilities
    - A defined approach to data management, its uniqueness and use of any tools available (e.g. Unique Data Tool).
    - Management of test environment and utilisation and support to ‘higher’ environments
    - Planning and delivery of releases in the path to production, including detailed feature management (feature switching) / branching strategy

- Support and testing for alignment with MBTP Strategic Route to Live (SR2L) pipelines and tooling, including any test refactoring as necessary

- Support for testing through all environments, including into production (and any live proving)

- Instigate, adopt and support of any innovation and improvement initiatives to include – increasing throughput, AI concepts, well defined and controlled configuration management, well architected designs and architecture, utilising cloud offerings such as AWS

- Bug and issue resolution (all testing stages and production) with traceability to root cause analysis and appropriate testing and extended regression tests as appropriate

- Support the Home Office with audit and quality assurance / plan processes and checks

4.6.2 Throughout the lifetime of the Contract, the Supplier will consider the following:

- Utilising an automation approach which includes provision of stubs, simulators and appropriate test data for all stages of testing. Using AI/innovations to automate tests

- SR2L equivalents

- Contribute to Service Management Readiness Testing (SMRT) and transition to live activities.

- The Supplier will also provide Root Cause Analysis if changes cause P1 incidents.

4.7 **Level 3 Support**

4.7.1 The Supplier will provide a Level 3 Managed Service (as per appendix B – MBTP Level 3 Support Requirements v1.6), comprising of highly skilled technical capabilities required for effective and efficient incident management, problem management, change and continual improvement along with associated skills and processes required for product application support, based on the ITIL framework and incorporating agile DevOps culture.

4.7.2 Level 3 are expected to collaborate with Level 1 and Level 2 as well as other teams and stakeholders as required to ensure the continued availability and high quality of products and services.

4.7.3 Level 3 are expected to provide 24x7 support (for P1 incidents only) to keep Atlas operational and recover from live service incidents.

4.7.4 The FE Level 3 Team is expected to support service transition activities alongside the FE Development Team and the HO Service Transition Manager. This will comprise of:

(a) Alignment with HO Service Transition processes

(b) Impact assessment and scoping

(c) Knowledge acquisition and transfer (from the FE development team to L2 and L3)

(d) ServiceNow configuration, which is used for Incident, Problem and Change Management

(e) Transition execution and management.

(f) Acceptance into live service operations

(g) Supporting in assessing security vulnerabilities

(h) Patching of supported services

4.8 **Team Structure**

4.8.1 HO DDaT portfolios, programmes and projects tend to follow Agile and Lean practices, so Atlas Shared Services resources need to be proficient at managing delivery in this context with appropriate design & control.

4.8.2 It is anticipated that the Supplier will develop strong collaborative working relationships with the existing HO DDaT programme/project teams and with the other suppliers supporting HO DDaT with whom the supplier will work – Business Architects/Analysts, User Centric Design, Solution Architects, Test Team, Release Mgt and Service Design & Transition.

4.8.3 The Supplier will develop a clear understanding of the aims and objectives of the HO DDaT programme/project they are working on, so that they can effectively support HO DDaT in terms of their day-to-day work and engagement with others.

4.8.4 Atlas is already in a business as usual state. Any Supplier will be expected to take responsibility for any code that has been, or is in the process of being, developed after a suitable transition and handover period with the incumbent.

4.8.5 The Outline Implementation Plan (Order Form attachment 3) shows a guide of roles and quantity of resources required by role. By the end of month 3 as defined in the Implementation Plan (Order Form attachment 3) the supplier will conduct a resource review with the Buyer to determine the appropriate level of cover for the remainder of the mobilisation period. The Supplier is encouraged to continually review the resource profile, and feed back to the Product Manager, to ensure an appropriate level of cover.

4.8.6 TUPE may apply to the procurement but the HO does not make any representations or warranties in this regard. Bidders should make their own enquiries and take their own view, including obtaining their own legal and professional advice as appropriate.

4.8.7 Roles at SFIA Levels 1, 2 and 7 are not required and are not to be included in the Tender.

4.8.8 Flexibility in resourcing is needed, including resource optimisation and an ability to scale resources up or down as appropriately, according to future changes to priorities and budgets.

4.8.9 For the purposes of mobilisation and transition, delay payments will apply (See Order Form attachment 2 part A). If, by the end of month 6 as defined in the Implementation Plan (Order Form attachment 3) the fixed core team is not fully onboarded, the Buyer reserves the right to apply a delay payment equivalent to

20% of the fixed mobilisation and transition cost. The Buyer will apply a 20% retention payment to monthly payments during mobilisation and transition in order to achieve this.

4.8.10 The Team will be structured into two components:

- A fixed core team which will be required through the duration of the contract:
  - The Buyer anticipates that at least once every 6 months of the Contract a review will take place to determine the correct level of resources covered under the fixed core team
  - The figure for this ITT has been determined to allow for fair comparison of Price across all Bidders.
- A surge capacity team:
  - For work required which would exceed the capacity of the Fixed Core Team.
  - This team would provide surge capacity up until the next review point.

4.8.11 The Supplier will be expected to manage the cost of roles transitioning where it is the Supplier who makes the decision to do the transition. Examples of this would be staff rotation or staff leaving the Supplier.

5. GENERAL REQUIREMENTS

5.1 **Location and working arrangements**

[redacted]

5.2 **Bring your own device (BYOD**)

[redacted]

5.3 **Working Hours**

5.3.1 A standard day is considered to be 7.5 hours (excluding lunch) and the Supplier is required to provide staff cover between the hours of 8am - 6pm. Out of hours is expected to provide staff cover 24/7.

5.3.2 The Supplier may be required to work outside the standard operational day in exceptional circumstances e.g. a failure of service. This will be agreed in advance.

5.3.3 The Supplier should submit timesheets at the end of the month to the Product Manager for approval clearly highlighting the unsociable hours worked. The timesheets will need to be approved by the Product Manager before Supplier can submit an invoice.

5.4 **Travel and Expenses**

5.4.1 All expenses will be paid as per the HO expense policy. The HO shall provide a copy of its expenses policy to the Supplier, which the Supplier shall abide by, or require agreement by the HO in advance for any expenses that do not fall within the HO expenses policy.

5.4.2 Any expenses payable by the HO shall be reasonable and be subject to the approval by the HO. The Supplier shall seek approval from the relevant HO assigned approver prior to undertaking Travel outside of the HO designated locations and only charge for such expenses once the costs have been approved by the HO.

5.5 **Cultural Fit & Knowledge Transfer**

5.5.1 Cultural Fit:

5.5.1.1 The Supplier shall adhere to the Civil Service values (https://www.gov.uk/government/publications/civil-service-code).

Knowledge Transfer:

5.5.1.2 The Supplier will work dynamically with MBTP designated staff to ensure that knowledge is transferred into MBTP at the earliest opportunity.

5.5.1.3 MBTP has a strategic aim to increase the number of civil servants in digital delivery roles and the Supplier will be expected to operate alongside civil servant team members undertaking all the core delivery team roles such as developers, content designers, interaction designers, user researchers, release managers etc.

5.5.1.4 The Supplier shall:

1. support the mutual exchange of knowledge and skills. MBTP is progressing towards becoming a product driven organisation and encourages knowledge and skills transfer from skilled suppliers to Civil Servants and equally in return. This includes methods, tools and learned experience.
2. work with a mix of other suppliers and Civil Servants across multidisciplinary teams, collaborating to achieve the organisational goals. Sharing knowledge as required in order to achieve the goals.
3. provide staff who will be integrated into teams long-term in order to increase domain knowledge and establish working relationships. Whilst completely recognising the need for individuals to progress and move on as suppliers have need to change people from time to time. We expect individuals moving on to be replaced with adequate handovers in place.

5.6 **Security, Security Clearance and Supplier Personnel**

5.6.1 Supplier personnel (and sub-contractors) must comply with HMG Baseline Personnel Security Standard (BPSS) [redacted] clearance.

[redacted]

5.6.3 The Supplier shall ensure that all systems are operated in such a manner to support HO DDaT compliance with HMG Security Policy Framework and HMG Baseline Personnel Security Standard.

5.6.4 The Supplier shall ensure that all appropriate NCSC guidance is followed.

5.6.5 The Supplier shall ensure protection of HMG information assets and accreditation of the solution where appropriate.

5.7 **Information Security Management**

5.7.1 The Supplier is required to comply with the following Security Architecture principles, all of the below must be reflected in the security management plan (annex S3 part A of Framework Schedule 4 – Annex 3)

A The Supplier must re-use existing security patterns wherever possible, if a pattern does not exist then the MBTP Security Architect assigned to the project will create one.

B The Supplier must ensure they use approved products and services or seek approval to use an alternative product wherever possible.

C The Supplier must work with the MBTP Cybersecurity team to get any new products or services risk assessed and approved.

D The Supplier must ensure that any changes to existing patterns are agreed with the MBTP Cyber Security team.

E The Supplier must use the agreed container and server images that will be shared by the Buyer.

F The Supplier must minimise the cyber threat footprint by patching in compliance with the MBTP Vulnerability Policy (see Section A)

G The Supplier must ensure all agreed events are logged to the MBTP SIEM Tool (Splunk).

H The Supplier must ensure that all code is vulnerability scanned using an approved static scanning tool.

I The Supplier must ensure that they reuse the approved testing and delivery pipelines.

J Application and service support must be through script-based fix, progressed through the delivery pipeline.

K The Supplier must ensure that they implement processes and practices to ensure that the need to logon to a production platform is only under exceptional circumstances.

L The Supplier must ensure they work closely with the MBTP Cyber Security Team to identify the level of security assurance required for each deliverable e.g. an IT health check or configuration review.

M Data in transit and at rest must be compliant with Home Office Cryptography standards, specifically:

(i) Data in Transit (security management annex):

(a) Data in transit MUST be protected by either of the following:

TLS at the application layer.
SSH at the application layer.
IPSec at the network layer.

(b) Data in transit classified SECRET or above MUST be encrypted using NCSC CAPS Assisted high grade cryptographic devices or software.

(c) Known usage of TLS versions before 1.2 MUST be reported to HOCS.

(ii) Data at rest:

(a) All user writable partitions on devices not physically secured such as servers or removable media MUST implement full disk encryption (FDE) to provide confidentiality and integrity of the data.

(b) FDE must utilise pre-boot authentication (PBA) as detailed by NIST.

(c) An authenticated encryption with associated data (AEAD) form of encryption MUST be used to ensure both confidentiality and integrity of the data at rest. This can be achieved using modes of operation such as EAX/CCM.

(d) Data at rest classified SECRET or above must be encrypted using NCSC CAPS approved High Grade Cryptographic devices or software.

(e) Data at rest classified SECRET or above must be encrypted using NCSC CAPS approved High Grade Cryptographic devices or software.

(f) When utilising Full Disk Encryption, data at rest that is classified OFFICIAL (including with the SENSITIVE caveat) must be encrypted using NCSC CAPS assisted devices or software.

(g) Where performing file or database encryption, OFFICIAL data at rest MUST utilise AES with a key length of at least 256 bits.

5.7.2 There will be regular engagement between the FE team and the MBTP Cyber Security Team. Continuous engagement between the teams is vital to ensure cyber security requirements and activities are fully understood by development teams and incorporated into implementation plans. The Atlas SWG is held on a monthly basis, it is mandatory that the FE team is represented at each meeting.

5.7.3 The Supplier will be expected to comply with the Security Management Developer document (Section A).

6. CONTRACT MANAGEMENT

6.1 **Mobilisation and Transition**

6.2 The Supplier will engage with the Buyer's assigned Buyer Authorised Representative, or nominated delegate, to audit compliance for the accuracy of the Contract and of the Deliverables and/or Documentation against the Services (prior to any invoicing).

6.3 The Supplier will nominate a named representative for the purposes of mobilisation and transition, who will be responsible for engaging with the Buyer's assigned Buyer Authorised Representative, or nominated delegate, during the mobilisation and transition phase.

6.4 At least 20 days prior to commencement, the Supplier shall provide a draft implementation plan (See Annex S1 of Framework Schedule 4 – Annex 3) for review by the Buyer.

6.5 **Statements of work (SoW)**

6.5.1 The Supplier shall provide SoW in a format that is agreed by the Buyer (see Section A and the Additional Annexes).

6.5.2 Statements of work will then be reviewed for approval by the Buyer.

6.6 **Reporting**

6.6.1 The Supplier will be required to complete and deliver the following monthly reports to the Buyer:

6.6.2 Resource Review: Complete a resource tracker which will identify the baseline forecast of resource consumption; actual resource consumption for the month;

updated forecast each month. This will allow tracking of resources and of progress towards capped T&M contract value.

6.6.3 Sprint reports with Goals/ Actuals/ Comments/ Story Burndown & key Deliverables

6.6.4 Deliverables & Milestones: Report on what deliverables and milestone were achieved in the month; for any missed deliverables or milestones the reasons for the delay, the mitigation, and the revised target date.

6.6.5 Benefits: summary of measurable benefits delivered.

6.6.6 Dependencies: Update on whether dependencies are being met; and impacts if they are not.

6.6.7 A monthly report alongside submission of the Acceptance Certificate which captures the following:

6.7 **For development team:**

(a) Management Highlights

(b) Operational Highlights

(1) Cycle Time Analysis

(2) Lead Time for Change

(3) Story Point Estimation

(4) Velocity metric

- Consider using story points to measure velocity or another suitable metric that can be adopted through a joint agreement

(5) Tickets and estimation summary

(c) Code quality

(d) KPI dashboard

(e) Breakdown of development effort by programme and key deliverables

(f) Benefits delivered

(g) Technical debt summary

(h) Cybersecurity and resilience overview

(i) Percentage of successful changes

(j) For Level 3, we have the below metrics, but further metrics will be required as the performance framework develops:

(1) Incident management report in relation to SLAs

(2) Availability

(3) API statistics, trends and volume analysis

(4) Dashboards monitoring backlog volume over time

(5) Developer and integration automation Effort: Planned v Actual for key deliverables

6.8 **Risks & Issues.**

6.9 **Next Reporting Period – Look Ahead**

6.10 **The monthly report will also include the latest Procurement metrics, which are updated from time to time.**

6.10.1 The Supplier will align with the Buyer for DORA metrics to allow the Buyer to review and discuss improvements using DORA metrics as the standard and reference points. The DORA metrics cover:

- Deployment frequency
- Cycle time
- Failed releases
- Time to restore service
- Lead time for Change

6.10.2 We expect the Supplier to report on performance metrics attached and the below:

(a) Stories per release

(b) Accessibility compliance

(c) Median lead time for change

(d) Data quality tbc

(e) Compliance to engineering standards

(f) Management of security vulnerabilities

(g) Collaboration with cyber security team / attendance at SWG

(h) Report on staff retention

(i) Opportunities taken to improve throughput

(j) Cost optimisation

(k) Mean time to resolution

6.10.3 Specifically the supplier will report on the following Key Performance Indicators (KPIs) (which are also outlined in Attachment 4):

Theme	KPI and rationale	Measurement and frequency	Targets
Code Quality	Maintain & Improve SonarQube Code coverage at AutoSIT: Ensures adherence to	SonarQube code coverage, Monthly	See table 6.6.11 for the Service Credits applied

	coding best practice, maintains code quality, and detects errors early for sustainable, reliable production.		
Testing	Functional Code failures in PRP 1 & 4 environments: Aims to minimise deployment failures in live environments (PRP1, PRP4). Pre-production code is highly integrated, and functional failures can slow down overall delivery and block the production pipeline.	P1/P2 failures in PRP1 and PRP4 environments per sprint across sprint teams of FE, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12
Lead Time to Change[1]	Lead time to change measures the average time it takes for a code change to be deployed to production: A shorter lead time indicates a faster and more efficient delivery process, enabling faster time to market and quicker response to customer needs.	Total lead time for all deployed changes / Number of deployed changes, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12
Cycle Time (dev)	Time it takes for a work item to get from the moment work starts (starting with 'In progress' status to when it is delivered 'Done' or 'Live'). *Tracking cycle time to restore pre transition, we can identify bottlenecks, optimise workflows, and improve overall productivity*.	Total cycle time for all completed items / no of completed items, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12
Deployment Frequency[1]	Frequent deployments to Production: Crucial for continuous delivery, ensuring frequent deployments that enhance agility, deliver quicker value to users and stakeholders, and provide more opportunities for feedback.	Deployments to Production per sprint across sprint teams of FE, Monthly	To be determined during onboarding in accordance with paragraph 6.6.12
Platform Stability in Production (failed change) [1]	Production Outages P1 or P2 because of FE code changes deployed in the last 5 working days (identified by through RCA): *Aims to minimise production outages to*	Number of outages by quarter across sprint teams of FE, Quarterly	See table 6.6.11 for the Service Credits applied

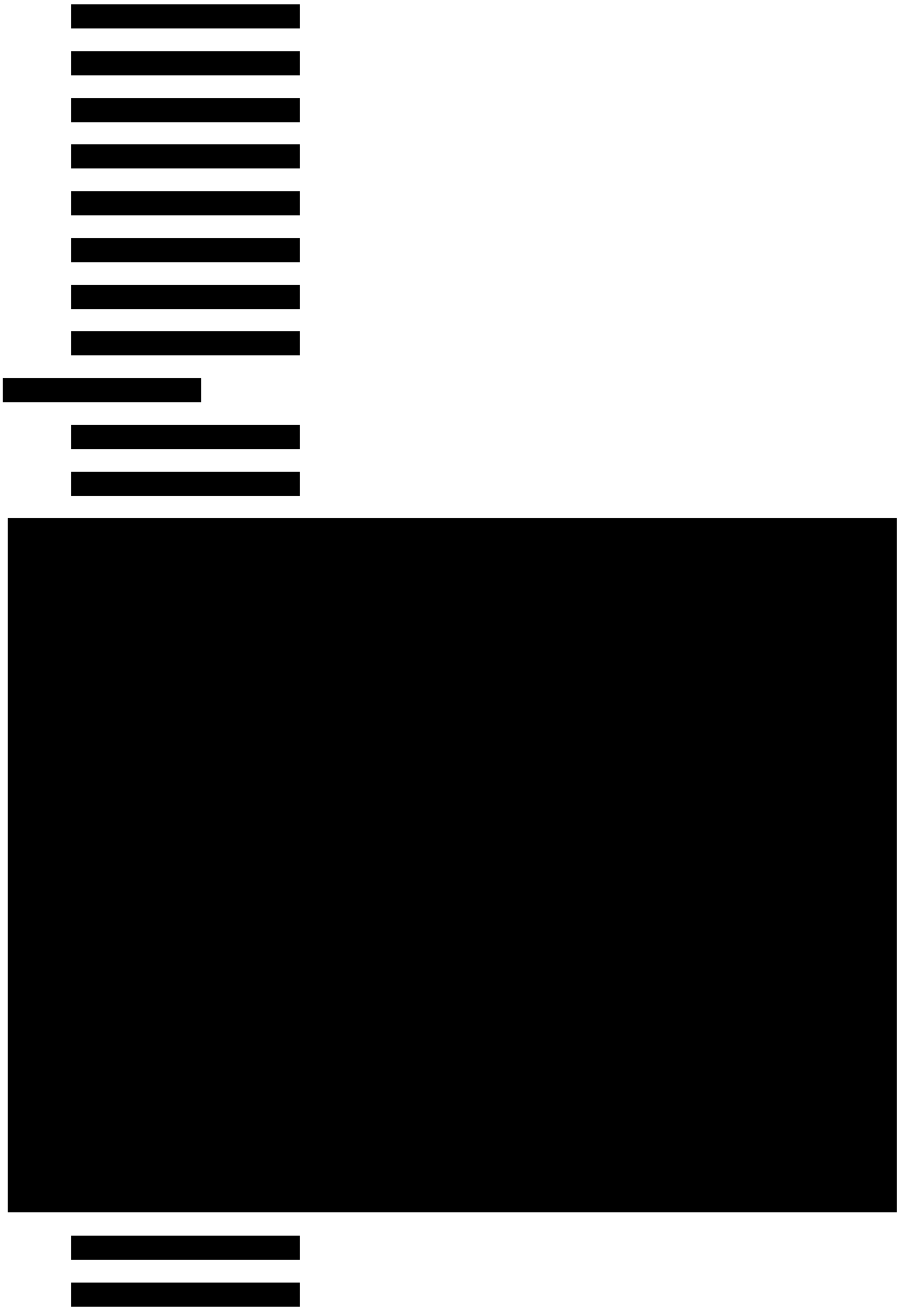
	enhance case worker productivity and product perception.		
Service Availability	The percentage of time a service is operational and available to users: It assesses the reliability and uptime of the service, ensuring it meets the (MBTP) (NFR).	Total uptime / (total uptime + total downtime), Monthly	99.9% availability, during core hours, excluding outages due to releases or environment unavailability (as outlined in Appendix B – Level 3 Support Requirements)
L3 Response Time	The efficiency and speed of responding within the team for P1, P2, P3, and P4: Tracking time to respond, we can identify bottlenecks, optimise workflows, and improve overall productivity	% of tickets responded to as per the SLAs in the Level 3 Requirements Document, from ticket assigned to FE to ticket closed, Monthly	<30 minutes for a P1 incident <30 minutes for a P2 incident <12 working hours/1.5 day for a P3 incident <24 working hours/3 days for a P4 incident (For further details, see Appendix B- Level 3 Support Requirements)
L3 Restoration Time[1]	The efficiency and speed of restoring services within the team for P1, P2, P3, and P4: Tracking time to restore, we can identify bottlenecks, optimise workflows, and improve overall productivity	% of tickets resolved as per the SLAs in the Level 3 Requirements Document, from ticket assigned to FE to ticket closed, Monthly	<4 hours for a P1 incident <8 hours for a P2 incident <24 working hours/3 days for a P3 incident <40 working hours/5 days for a P4 incident (For further details, see Appendix B- Level 3 Support Requirements)
L3 Restoration Time[1]	The efficiency and speed of restoring services within the team for P1 and P2: Tracking time to restore, we can identify bottlenecks, optimise workflows, and improve overall productivity	% of tickets resolved as per the SLAs in the Level 3 Requirements Document, from ticket assigned to FE to ticket closed, Monthly	<4 hours for a P1 incident <8 hours for a P2 incident (For further details, P3 & P4 resolution requirements, and required responses times, see Appendix

			B- Level 3 Support Requirements)
Social Value	Tackling economic inequality: Create employment and training opportunities particularly for those who face barriers to employment and/or who are in deprived areas, and for people in industries with known skills shortages or in high growth sectors	Number of full-time equivalent (FTE) employment opportunities created under the contract, by UK region, Yearly	To be determined during onboarding in accordance with paragraph 6.6.12
Social Value	Equal opportunity: Increase representation of disabled people and tackling inequality in the contract workforce	Total percentage of full-time equivalent (FTE) disabled people employed under the contract, as a proportion of the total FTE contract workforce, by UK region, Yearly	To be determined during onboarding in accordance with paragraph 6.6.12

[1] These are KPIs that map back to the DORA metrics.

[redacted]

[redacted]



7. GOVERNANCE

7.1 There will be four categories of governance meetings to review the performance of the Services which the Supplier shall attend. The occurrence of operational management and contract management meetings may be more frequent during the commencement of Services.

7.1.1 operational management meetings, which will include:

7.1.2 meet weekly, attended by the Supplier's delivery manager.

7.1.3 attend multiple delivery meetings

7.1.4 programme delivery boards, steering groups and change boards to explain impact assessments, if necessary review operational delivery; and

7.1.5 address risks, mitigations and escalations

7.1.6 contract management (Monthly Balanced Scorecard Meetings) which will:

7.1.7 meet monthly, attended by the Supplier's Contract Manager.

7.1.8 review the Supplier's performance against key performance indicators (Performance Monitoring Reports), Statements of Work, the burn rate against Contracts, and operational delivery; and

7.1.9 An example balanced scorecard can be found in the additional annexes.

7.1.10 It is split into four categories:

(a) **Performance to pay process:** Measured by ensuring that all inputs (timesheets, supplier reports and acceptances certificates etc) are submitted in accordance to performance to pay process timescales

(b) **Service requests and product centricity:** Measurement will include a 10-day target for all services that are requested and SOWs are rejected if they have insufficient information or quality.

(c) Delivery, partnering behaviours and value add: Measured by project outputs that are detailed in SOW, such as outputs completed within the stated timelines and identified value add activities

(d) **People (resourcing and people in place for delivery):** Measured by having no issues with the quality of the work that is being delivery, and no skill deficiencies

(e) Measure that are to be monitored in the meetings

- Resource cost variance
- Start date variance
- Training hours
- Performance to pay process
- Quality – service resourcing
- Quality – tasking efficiency

- Quality – technical alignment
- Partnering
- Added value
- Improve – value add

7.2 Architecture, engineering and Technical Design Authority meetings, which will:

7.3 be scheduled as required, attended by portfolio CTO team, supplier leads, delivery manager to review architecture, technology and engineering efficiencies.

7.4 **Change Control**

7.4.1 The change control procedure is as per the RM6100 Framework Terms and Conditions.

7.5 Standards and Policies - See Section A.

7.6 **Continuous Improvement**

7.6.1 See annex S7 of Framework Schedule 4 – Annex 3.

7.7 **Business Continuity & Disaster Recovery**

7.7.1 “Business Continuity and Disaster Recovery” means any activities that support the continuous running of an organisation during a major accident (fire, flooding, or any other natural disasters, explosion, electrical fault, major health epidemic/pandemic or geopolitical events which may have an impact on a business and/or services provided)

7.7.2 Teams providing AWS cloud-based autoscaling infrastructure within the EBSA hosted platform will need to maintain an awareness of cross-cutting business continuity and disaster recovery requirements across DDaT to ensure critical IT services, data and business operations are restored as quickly as possible after an unexpected event.

7.7.3 From time to time, MBTP will validate their BC/DR plans and the Supplier will provide support into the operational teams, specifically failover testing and rehearsals of operational procedures.

7.7.4 See Annex S6 of Framework Schedule 4 – Annex 3 for further information

7.8 **Exit Management**

7.8.1 The Supplier shall work closely with the Buyer to support the on-boarding, transition, due diligence and knowledge transfer activities. This will be an ongoing process, and not confined to the Contract exit provisions or the below requirements.

7.8.2 Planning

7.8.2.1 The Supplier shall:

7.8.2.2 be required to work closely with the Buyer to support the exit and transition from the contract including support for new services and the transfer of operational knowledge and ensuring all documentation is up to date.

7.8.2.3 provide a dedicated exit manager to deliver the exit transition plan and deliverables therein.

7.8.2.4 provide an exit transition plan no less than 6 months before contract end that will include but not limited to.

- An exit transition plan in an agreed format
- A timetable of events
- Resource plan
- Assumptions
- Activities
- Responsibilities
- Risks

7.8.3. Licences

7.8.3.1. Three (3) months prior to expiry or within one (1) weeks' notice of termination of this Agreement the Supplier shall deliver to the Buyer all licences for Software used in the provision of Services which were purchased by the Buyer.

7.8.3.2. On notice of termination of this Agreement the Supplier shall, within one (1) week of such notice, deliver to the Buyer details of all licences for Supplier Software and Buyer Third Party Software used in the provision of the Services, including the terms of the software licence agreements. For the avoidance of doubt, the Buyer shall be responsible for any costs incurred in the transfer of licences from the Supplier to the Buyer or to a Replacement Supplier provided such costs shall be agreed in advance. Where transfer is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

7.8.3.3. Within one (1) month of receiving the software licence information as described above, the Buyer shall notify the Supplier of the licences it wishes to be transferred, and the Supplier shall provide for the approval of the Buyer a draft plan for licence transfer, covering novation of agreements with relevant software providers, as required. Where novation is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

7.8.3.4. Licences includes any item that can be classified as being Intellectual Property (IP). All IP & IPR is owned by MBTP and IP items within the Supplier's domain in relation to the operational running of the BDPT service must be transferred to MBTP within the Exit Plan. IPR is as defined in the call off terms.

7.8.4. Knowledge Transfer

7.8.4.1. On request the Supplier shall provide to the Buyer an analysis of the volumetrics (or other measure(s) of usage) of the Services to the extent reasonably necessary to enable the Buyer to plan migration of such workload to a new supplier provided always that this analysis involves

providing performance data already delivered to the Buyer as part of the performance monitoring regime.

7.8.4.2. The Supplier shall provide such information as the Buyer reasonably considers necessary for the actual Replacement Supplier, or any potential Replacement Suppliers during any re-procurement process, to define the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.

Section A – Guidance, Standards and Policy References

Suppliers will be expected to adhere to the following Government and Departmental Processes, Policies and Standards, working closely with 3rd party teams to achieve them:

Security and Risk Management		
No.	Document	Link
1	Government Security & Cyber Policies	Policy - UK Government Security - Beta
2	Government Security Classification Policy	Government Security Classifications - GOV.UK (www.gov.uk)
3	Security and Privacy Controls for Information Systems and Organizations	SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)
4	Home Office Departmental Cyber Security Strategy 2023 – 2025	Included in additional annexes
5	Home Office Cyber Security Patching Policy	Included in additional annexes
6	Home Office Cyber Security Technical Vulnerability Management Standard	Included in additional annexes
7	HMG Security Policy Framework	Security policy framework - GOV.UK (www.gov.uk)
8	National Cyber Security Centre Guidance	All topics - NCSC.GOV.UK
10	National Cyber Security Centre (NCSC) Cyber Assessment Framework v3.2	Microsoft Word - Cyber Assessment Framework V3.2 (ncsc.gov.uk)
11	Security Management (Developer)	Included in additional annexes
12	End User Device Agreement	Included in additional annexes
13	Offshoring Policy	Included in additional annexes

Technical Standards and Governance		
No.	Document	Link
1	Guidance for developing new API's	API technical and data standards - GOV.UK (www.gov.uk)
2	Home Office Engineering and Development Standards	https://engineering.homeoffice.gov.uk/
5	Release Management Process	Included in additional annexes
6	SRE Guidance and standards	Included in additional annexes
7	SRE Guidance and standards: Availability	Included in additional annexes
8	SRE Guidance and standards: Monitoring	Included in additional annexes
9	SRE Guidance and standards: Logging	Included in additional annexes
10	SRE Guidance and standards: New Security Controls	Included in additional annexes

Project Management and Delivery		
No.	Document	Link
1	Greening IT Strategy	Greening government: ICT and digital services strategy 2020-2025 - GOV.UK (www.gov.uk)
2	Home Office Digital & Technology Strategy	Government Cyber Security Strategy: 2022 to 2030 - GOV.UK (www.gov.uk)
3	Accessibility Guidance	Included in additional annexes
4	Balanced Scorecard	Included in additional annexes
5	SOW Sample	Included in additional annexes
6	Performance Metrics	Included in additional annexes

Appendix B - Level 3 Support Requirements

Level 3 Support Requirements Summary

Provision of a Level 3 Managed Service, comprising of highly skilled technical capabilities required for effective and efficient incident management, problem management, change, and continual improvement, along with the associated skills and processes required for product application support, based on the ITIL framework and incorporating agile DevOps culture.

Level 3 are expected to collaborate with Level 1 and Level 2 as well as other teams and stakeholders as required to ensure the continued availability and high quality of products and services.

1 Incident Management

1.1 Requirement description
The purpose of the Incident Management process is to restore agreed service to the business as soon as possible following an unplanned event which resulted in a loss of service.

1.2 Requirement outcome
Service restoration or recovery from unplanned interruption to a product, or a reduction in the quality of service, or an event that has not yet impacted the service according to agreed incident management process.

1.3 Requirement key activities and deliverables
- Supporting incident management and associated processes
- Resolving incidents to agreed SLAs
- Collaborating with other teams on incident management
- Communicating incident progress updates to stakeholders
- Restoration of normal service operation
- Responding to automated event notifications raised through monitoring
- Primary engagement via ServiceNow and JIRA

1.4 Requirement criteria
Incident Management SLAs:

P1 - P1 means an incident:
a) that results in a complete or substantial loss of the product; or
b) that results in an essential part of the product being unusable for all end users; or
c) that results in all End Users being unable to access the product

P2 - P2 means an incident:
a) where the product is materially adversely affected but can be circumvented; or
b) where the product remains operable but certain material aspects of the product are disabled; or
c) where a large group of End Users is unable to access the Service; or certain material aspects of the product

P3 - P3 means an incident:
a) that results in a minimal business impact for the product where non-critical functions or procedures are down, unusable, or difficult to use; or
b) affecting a single or small group of end users

P4 - P4 means an incident:

a) that results in little or no material impact on the product or the customer's business; or
b) where the product is determined to be functioning as designed but the Incident may result in a Change Request to modify or enhance the product; or
c) raised in response to questions, compliments, complaints, escalations or queries from the customer.

However, if a code fix is required then this the following apply, but will depend on the severity of the incident and will be pragmatically allocated to a sprint:

- Severity 1 & 2 incidents - hot fixed outside Release activity
- Severity 3 Incident - allocated to either of the next 2 Releases
- Severity 4 Incident - allocated to any of the next 3 Releases
- Severity 5 Incident - allocated to any of the next 4 Releases

This provides the team with the ability to allocate a fix to a Release, where a code fix is required to provide a resolution. If a workaround is available, then the incident will be closed, and a problem ticket can be created to provide a permanent resolution. The metrics below can also be found within Attachment 4 and Appendix A – Specifications paragraph 6.6.10.

2 Problem Management

2.1 Requirement description
The purpose of the Problem Management process is to manage the lifecycle of all problems and to minimise the adverse impact of incidents and problems. The process will seek to reduce reoccurring incidents and reduce the impact of incidents that cannot be prevented. The process will react to incidents, events and problems once they have occurred, been raised or escalated to the problem manager.

2.2 Requirement outcome
Investigation and resolution of the root causes of incidents and thus minimisation of the adverse impact of incidents caused by errors within the supported environment, and prevention of incident recurrence related to these errors according to agreed incident management process.

2.3 Requirement key activities and deliverables

- Performing a Root Cause Analysis (RCA) and collaborating with other teams during this process
- Resolving the root cause of incidents
- Developing workarounds until the "fix" can be released to production

2.4 Requirement criteria
Problem management supports Incident Management, seeking to eliminate the root causes of recurring incidents. Incidents and problems will be managed in accordance with the incident and problem management processes as defined by the product owner.

The team will adopt a proactive approach to Problem Management, seeking to resolve known errors and eliminate the root causes of recurring incidents, with the goal of driving down the volume of incidents against a baseline over time.

To this end, the team will undertake one-time Incident analysis to identify Problem management candidates and will continue this through the course of the agreement. From the resulting problem management candidates the team will take appropriate action, including but not limited to:

- Elaborating and delivering stories to eliminate root causes of known errors
- Elaborating and delivering stories to optimise the supported application functionality
- Non-technical activities in collaboration with MBTP's other delivery partners to improve processes etc.

Measurement of the success of proactive problem management will be reported through enhanced reporting in the monthly service performance pack, reviewed at the monthly Service Review Board.

3 Change Management

3.1 Requirement description
The purpose of Change Management is to manage the approval and development of new business requirements, in collaboration with the Change Advisory Board (CAB).

3.2 Requirement outcome
Elaboration and delivery of requirements that deliver new or changed product functionality, according to agreed change management and delivery processes and supported by change augmentation resources as required.

3.3 Requirement key activities and deliverables
- Development of new business requirements, which have been approved by the Change Advisory Board (CAB)
- Supporting the progression of code through PRPx environments, in collaboration with Quality Assurance Testing (QAT)

3.4 Requirement criteria
Changes to be agreed at the Change Advisory Board (CAB). Changes will be managed in accordance with the Change Management process, as agreed by the product owner, and will be allocated to the team following CAB approval. As new requirements arise changes are requested by the product owner, added to the backlog and prioritised.

Each sprint typically results in a release candidate, which is delivered to testing and for deployment through non-production and production environments. Completed work will be rolled into releases. The team will provide support for a production release. In order to ensure that changes are aligned with DDaT strategy and represent value for money. Demand will be managed and change will be governed by a Change Advisory Board (CAB).

Changes shall be categorised in three types:
1. Minor changes
2. Non-minor changes
3. Standard changes

Minor Change definition:
- Any level of urgency
- Marginal service impact (i.e. change is related to a single application and side-effects can be safely excluded)
- Low risk
- Non-epic

Non-minor Change definition:

- Any level of urgency
- Substantial service impact (i.e. change affects several applications, change affects fundamental parts of the infrastructure, supporting several applications
- Medium risk
- Epic

Standard Change:
- Are pre-approved and require no additional assessment and authorisation;
- Defined per the definition of “minor changes” with the additional criterion that they are repeatable tasks that can be executed according to a standardised work instruction.

4 Availability Management

4.1 Requirement description
The purpose of the Availability Management process is to minimise unplanned unavailability. This is achieved by reporting the actual availability against the planned availability, identifying risks to availability and recommending opportunities to improve availability.

4.2 Requirement outcome
Proactive management and maintenance of the product to ensure availability expectations/SLAs are met.

4.3 Requirement key activities and deliverables
- Ensuring reliability, maintainability and resilience of the product, together contributing to the availability of the service
- Promote the use of serverless computing, scalable micro-services, automated provisioning, monitoring and self-healing, allowing for a product to be almost always available
- Availability testing, the almost limitless availability of Cloud services provides the ability to test this availability using manual or automated test techniques
- Focus on automation, which largely reduces the need for manual approaches.

4.4 Requirement criteria
99.9% product availability, during core hours, excluding outages due to releases or environment unavailability.

As outlined in Attachment 4 and in Appendix A – Specifications paragraph 6.6.10, the team will provide products, including appropriate proactive monitoring and maintenance, to attain 99.9% availability of the Production environment, this is limited to the application and in collaboration with the teams supporting the peripheral systems.

The team will document and improve the proactive maintenance plan, for the application, on an ongoing basis, this will be shared with the product owner and could be in the form of a backlog.

5 Release and Deployment Management

5.1 Requirement description
The purpose of the Release & Deployment Management process is to ensure that standardised methods and procedures are used to handle releases into production in an efficient and prompt manner.

5.2 Requirement outcome
Preparation and testing of release packages and support for deployment across non-production and production environments.

5.3 Requirement key activities and deliverables
- Documented Release and Deployment process for the product
- Transition of release and deployment processes from delivery to live
- Supporting deployment to production if required

5.4 Requirement criteria
Release process and cadence to be agreed with Release Management and the product owner.

6 Environment Management

6.1 Requirement description
Proactive management and maintenance of the products in non-production environments to ensure availability expectations/SLAs are met, where agreed.

6.2 Requirement outcome
Proactive management and maintenance of the product in non-production environments to ensure availability expectations/SLAs are met

6.3 Requirement key activities and deliverables
- Ensuring non-production environments dedicated to the product are maintained
- Resolution of incidents associated with the agreed non-production environments
- In collaboration with EBSA to ensure alignment with strategic environment management initiatives

6.4 Requirement criteria
The team will be responsible for managing the agreed non-production environments dedicated to product, ensuring unimpeded development activity. This will be through the efficient resolution of tickets reporting environment issues and appropriate proactive maintenance of these environments. This will be in collaboration with EBSA to ensure alignment with strategic environment management initiatives.

7 Service Level Management

7.1 Requirement description
The purpose of Service Level Management is to define, document, agree, monitor, measure, report and review the level of IT services.

7.2 Requirement outcome
The supplier will advise and assist in the definition, documentation, agreement, monitoring, measuring, reporting and review of Service Level Agreements (SLAs).

7.3 Requirement key activities and deliverables
- Monthly Service Management review
- Ensuring the agreed SLAs are delivered
- Triage of allocated tickets
- Provision of agreed services during change freeze or furlough periods
- Agreed governance model

7.4 Requirement key activities and deliverables
To be defined dependent upon the needs of the product and in agreement with the product owner.

8 Continual Improvement

8.1 Requirement description
The identification and implementation of improvements to the product resulting in improved service quality and enables a product to change to meet the evolving needs of the business.

8.2 Requirement outcome
Identification and implementation of improvements to the product as agreed with the product owner.

8.3 Requirement key activities and deliverables
• Product innovation candidates provided by the supplier to the product owner and delivered by the supplier

8.4 Requirement criteria
Prioritised by the product owner or delegate as part of the change backlog.

9 **Out of Hours Support**

9.1 Requirement description
Provision of an Out of Hours (OOH) service, managing agreed incidents outside of core service hours.

9.2 Requirement outcome
The supplier will provide Out of Hours support for the product when required.

9.3 Requirement key activities and deliverables
• Core support hours are 0900 to 1730 (excluding Bank Holidays) Monday to Friday, support outside of these hours is classed as OOH
• Appropriately skilled resources will be on “Standby” during the OOH period, to respond to the agreed incidents

9.4 Requirement criteria
To be defined dependent upon the needs of the product in agreement with the product owner.

10 Product and Service Management

10.1 Requirement description
Product and service management capability will ensure the effective and efficient management of all aspects of the product and live service.

10.2 Requirement outcome
Ensure SLAs are met, the quality of the product and service are continually high, all aspects of the product and live service are managed effectively and efficiently.

10.3 Requirement key activities and deliverables
• Manage all aspects of the product to ensure SLAs are met and the quality of the product and live service are continually high
• Collaborate with other teams to ensure the smooth running of the estate and shared products

10.4 Requirement criteria
Suitably skilled product and service managers need to manage all aspects of the product at all stages of the lifecycle.

11 Transition Management

11.1 Requirement description
Working collaboratively with the product team and the transition team to establish the required L3 provision and complete transition to the designated lifecycle phase and/or team.

11.2 Requirement outcome
Support the Home Office to transition support to another team. It will be the responsibility of the Home Office to provide appropriately skilled resource to lead the transition. The supplier will support transition by providing documentation, participating in knowledge transfer sessions, pair programming and working with members of the designated team. The supplier will work with the Home Office to define transition timelines during the duration of the agreement.

11.3 Requirement key activities and deliverables
- Development of a transition plan
- Due diligence and baselining of the service
- Complete mobilisation, clearance and knowledge acquisition
- Support MBTP's Service Transition team with required artefacts and governance

11.4 Requirement criteria
Support transition when requested by the product owner.

12 "Shift Left"

12.1 Requirement description
Transferring the incident management workload from Level 3 to Level 1 and Level 2 so that Level 1 and Level 2 can fix issues without the intervention of Level 3.

12.2 Requirement outcome
Activities to transfer incident management workload from Level 3 support to Level 1 and Level 2.

12.3 Requirement key activities and deliverables
- "Shift Left" activity, focussing on transferring knowledge and skilled ability to fix incidents to the Level 1 and Level 2 teams

12.4 Requirement criteria
Knowledge sharing, knowledge transfer, upskilling, and the writing of knowledge articles and work instructions.

Appendix C –Additional Reporting, Value Add and Social Value Bid Commitments