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 June 2021 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 – Outline 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;
12. Annex 1 – Tech Debt
13. Annex 2 – Governance and Forums;
14. Annex 3 – Supplier’s Response (the tender submitted by the Supplier to Buyer as part of the ITT proposal in response to the Buyer's invitation to tender entitled "Lot 2: Border Platforms and Services” Contract under Framework RM6100 Technology Services 3 (“Supplier’s Response”);
15. Annex 4 - Call Off Terms and Additional/Alternative Schedules and Clauses; and
16. Annex 5 – Product List.

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

Crown Commercial Service

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

1.1.2 the Order Form;

1.1.3 Any Statement of work

## Section A
## General information

| **Contract Details** | |
|---|---|
| **Contract Reference:** | C9667-B |
| **Contract Title:** | Crossing the Border Products and Services |
| **Contract Description:** | Provision of a managed service to provide the run, maintain and sustain Border Platform services. |
| **Contract Anticipated Potential Value:** this should set out the total potential value of the Contract | £25,900,000 |
| **Estimated Year 1 Charges:** | [redacted] |
| **Commencement Date:** this should be the date of the last signature on Section E of this Order Form | 04/12/2025 |

| **Buyer details** |
|---|
| **Buyer organisation name**<br>Secretary of State for the Home Department, acting on behalf of the Home Office (referred to as "Buyer") |

Crown Commercial Service

**Billing address**
Your organisation's billing address - please ensure you include a postcode
Home Office Shared Service Centre
[redacted]

**Buyer representative name**
The name of your point of contact for this Order
[redacted]

**Buyer representative contact details**
Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
[redacted]

**Buyer Project Reference**
Please provide the customer project reference number.
C9667-B

**Supplier details**

**Supplier name**
The supplier organisation name, as it appears in the Framework Agreement
Kainos Software Limited

**Supplier address**
Supplier's registered address
[redacted]

Crown Commercial Service

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

**Supplier representative contact details**
Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
[redacted]

**Order reference number or the Supplier's Catalogue Service Offer Reference Number**
**ITT_77424**
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.

**Guarantor details**
*Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.*

**Guarantor Company Name**
The guarantor organisation name

Not Applicable

**Guarantor Company Number**
Guarantor's registered company number

Not Applicable

**Guarantor Registered Address**
Guarantor's registered address

Not Applicable

## Section B
## Part A – Framework Lot

**Framework Lot under which this Order is being placed**
*Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the Buyer is procuring technology strategy & Services Design in*

Crown Commercial Service

*addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.*

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

## Part B – The Services Requirement

**Commencement Date**
See above in Section A

**Contract Period**
*Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:*

| Lot | Maximum Term (including Initial Term and Extension Period) – Months (Years) |
|---|---|
| **2** | 36 (3) |
| **3** | 60 (5) |
| **5** | 60 (5) |

**Initial Term** Months
48 Months

**Extension Period (Optional)** Months
12 months

**Minimum Notice Period for exercise of Termination Without Cause** 6 Months
(183 Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Crown Commercial Service

**Sites for the provision of the Services**
*Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.*

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

[redacted]

**Supplier Premises:**
Kainos Premises below or remotely:

[redacted]

**Third Party Premises:**

AppVia Premises or remotely:

[redacted]

Crown Commercial Service

ScrumConnect Premises or remotely:

[redacted]

**Buyer Assets**
*Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms*
Home Office POISE Laptops

**Additional Standards**
Guidance *Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*

Additional standards will be agreed by the Parties, acting reasonably, prior to the start of the Implementation Period.

**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.*

[redacted]

Crown Commercial Service

**Buyer ICT Policy**

[redacted]

**Insurance**
*Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.*

Third Party Public Liability Insurance (£) - £5,000,000

Professional Indemnity Insurance (£) - £1,000,000 and in the annual aggregate

**Buyer Responsibilities**
*Guidance Note: list any applicable Buyer Responsibilities below.*

Please find below the dependencies on the Buyer for the Border Platforms Discovery and Mobilisation Period of 8th December 2025– 30th June 2026.

A full list of dependencies for the Implementation Period will be agreed by the Parties, acting reasonably, prior to the start of the Implementation Period.

Annual check points will be undertaken throughout the contract lifecycle where the outcomes of the following year will be agreed. These are referred to in this Order Form as Annual Service Conformance Reviews.

The first Annual Service Conformance Review is February 10th 2027, approximately seven months after the end of the Discovery and Mobilisation period. In addition to Annual Service Conformance Reviews, the Parties will meet monthly to review Supplier performance and once every three months during the Implementation Period to establish if the agreed scope of services still meets the Buyer's needs or whether the Change Request process shall be followed pursuant to Schedule 5 (Change Control Procedure).

The Buyer will meet the following responsibilities listed in the table below. In the event that any of these Buyer Responsibilities are not met then:

Crown Commercial Service

The Supplier is relieved from liability for achieving the affected deliverables by the relevant due dates; and

The Parties shall, acting reasonably, agree on adjustment to dates, deliverables or financial envelope as applicable

[redacted]

**Goods**
*Guidance Note: list any Goods and their prices.*
Not Applicable

**Governance – Option Part A or Part B**
*Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.*

| Governance Schedule | Tick as applicable |
|---|---|
| Part A – Short Form Governance Schedule | ☐ |
| Part B – Long Form Governance Schedule | X |

Crown Commercial Service

The Part selected above shall apply this Contract.

**Change Control Procedure – Option Part A or Part B**
*Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.*

| Change Control Schedule | Tick as applicable |
|---|---|
| Part A – Short Form Change Control Schedule | ☐ |
| Part B – Long Form Change Control Schedule | X |

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

[redacted]

## 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 | X |
| S2: Testing Procedures | X |
| S3: Security Requirements (either Part A or Part B) | Part A ☐ or Part B X |
| S4: Staff Transfer | X |
| S5: Benchmarking | X |
| S6: Business Continuity and Disaster Recovery | X |
| S7: Continuous Improvement | X |
| S8: Guarantee | ☐ |
| S9: MOD Terms | ☐ |

**Part B – Additional Clauses**
*Guidance Note: Tick any applicable boxes below*

| Additional Clauses | Tick as applicable |
|---|---|
| C1: Relevant Convictions | X |

Crown Commercial Service

| | |
|---|---|
| C2: Security Measures | X |
| C3: Collaboration Agreement | X |

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**
*Guidance Note: Tick any applicable boxes below*

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.

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

**Additional Schedule S3 (Security Requirements)**
*Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.*

[redacted]

**Additional Schedule S4 (Staff Transfer)**
*Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.*

The Buyer's liability for redundancy costs will be as detailed in Part B Annex 1 (Redundancy Costs) of the attached Staff Transfer Schedule and will be apportioned for Lot 2 and Lot 3 in scope Individuals as appropriate by the Buyer.

During the contract engrossment period, the incumbent supplier identified two (2) individuals who are in scope that were not identified prior to ITT release. Further details are set out in the attached Data Share document below.

Crown Commercial Service


S4 Staff Transfer .docx


Data Share

**Additional Clause C1 (Relevant Convictions)**
*Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.*
Additional Clause C1 (Relevant Convictions)

Participation in a criminal organisation
- Participation offence as defined by section 45 of the Serious Crime Act 2015
  - Conspiracy within the meaning of:
  - section 1 or 1A of the Criminal Law Act 1977; or
  - article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983, where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA on the fight against organised crime.

Corruption
- Corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906;
- The common law offence of bribery;
- Bribery within the meaning of sections 1, 2 or 6 of the Bribery Act 2010, or section 113 of the Representation of the People Act 1983.

Terrorist offences or offences linked to terrorist activities
- Any offence:
  - listed in section 41 of the Counter Terrorism Act 2008;
  - listed in schedule 2 to that Act where the court has determined that there is a terrorist connection;
  - under sections 44 to 46 of the Serious Crime Act 2007 which relates to an offence covered by the previous two points.

Money laundering or terrorist financing
- Money laundering within the meaning of sections 340(11) and 415 of the Proceeds of Crime Act 2002
- An offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996.

Child labour and other forms of trafficking human beings
- An offence under section 4 of the Asylum and Immigration (Treatment of Claimants etc.) Act 2004;
- An offence under section 59A of the Sexual Offences Act 2003
- An offence under section 71 of the Coroners and Justice Act 2009;

Crown Commercial Service

- An offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994
- An offence under section 1, 2 or section 4 of the Modern Slavery Act 2015.

Non-payment of tax and social security contributions

- Breach of obligations relating to the payment of taxes or social security contributions that has been established by a judicial or administrative decision.
- Where any tax returns submitted on or after 1 October 2012 have been found to be incorrect as a result of:

o HMRC successfully challenging the Supplier under the General Anti – Abuse Rule (GAAR) or the "Halifax" abuse principle; or

o a tax Buyer in a jurisdiction in which the Supplier is established successfully challenging it under any tax rules or legislation that have an effect equivalent or similar to the GAAR or "Halifax" abuse principle;

o a failure to notify, or failure of an avoidance scheme which the Supplier is or was involved in, under the Disclosure of Tax Avoidance Scheme rules (DOTAS) or any equivalent or similar regime in a jurisdiction in which the Supplier is established.

Other offences

- Any other offence within the meaning of Article 57(1) of the Public Contracts Directive as defined by the law of any jurisdiction outside England, Wales and Northern Ireland.
- Any other offence within the meaning of Article 57(1) of the Public Contracts Directive created after 26th February 2015 in England, Wales or Northern Ireland.

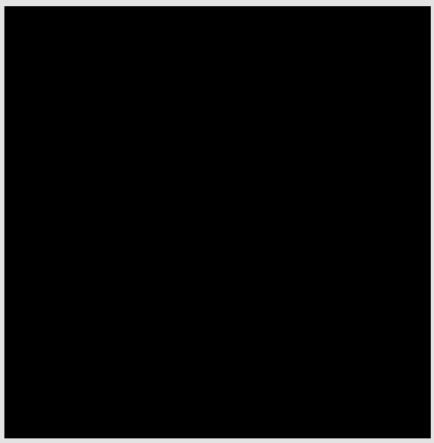
**Additional Clause C3 (Collaboration Agreement)**

*Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.*

[redacted]

Kainos

Crown Commercial Service



The Supplier will work with the Service Integrator Supplier and other Suppliers in the CtB ecosystem to agree and execute the Collaboration Agreement which will be delivered to the Buyer within the first thirty (30) Working Days from the Contract Commencement Date

## 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.*

Commercial rates and any negotiated discounts, together with any prices set out in the Contract or Statement of Work(s). Any personal data pertaining to the Supplier's personnel. The Supplier's Response, including but not limited to, methodologies and approaches.

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

**For and on behalf of the Supplier**

| | |
|---|---|
| Name | [redacted] |
| Job role/title | |
| Signature | |
| Date | |

**For and on behalf of the Buyer**

| | |
|---|---|
| Name | [redacted] |
| Job role/title | |
| Signature | |
| Date | |

Crown Commercial Service

## Attachment 1 – Services Specification

This Attachment 1 (Service Specification) sets out the Services as defined in the Buyer's ITT. The Supplier's Response to the Buyer's ITT is set out in Annex 3 (Supplier's Response). In addition, throughout the contract engrossment period, the Parties have agreed the following:

- updated Charges as per Attachment 2 (Charges and Invoicing);
- an updated outline implementation plan detailing how transition will take place from the incumbent provider to the Supplier (the "Transition Plan") in Attachment 3 (Outline Implementation Plan); and
- an updated Product List in Annex 5 (Product List).

### 1. PURPOSE

1.1 The purpose of this procurement is for the Buyer to procure Platforms and Systems Architecture Management Services to provide the detailed services outlined in this Lot 2 document for the initial contract term of 4 years with the option to extend for a further period of one year (4 + 1).

### 2. BACKGROUND OF THE BUYER

The first duty of the Government is to keep citizens safe and the country secure. The Home office plays a fundamental role in the security and economic prosperity of the UK. Further detail can be accessed here. Home Office - GOV.UK (www.gov.uk)

2.1 The Buyer is the lead government department for immigration and passports, drugs policy, crime, fire, counterterrorism, and police. The objectives, and priorities of the department can be found here.

https://www.gov.uk/government/organisations/home-office/about

2.2 Within the Home Office, Home Office Chief Operating Office Group, the Home Office Digital Directorate provides the Buyer's internal and external IT and digital services. The strategy and principles of the directorate can be found here;

Home Office 2030 Digital Strategy (accessible) - GOV.UK

2.3 Home Office Digital support the Home Office vision through being a government-leading digital department with in-house specialist skills, building solutions for the rest of the Home Office that will enable its objectives. The Home Office 2030 Digital Strategy sets out a vision for transforming the department's Digital capabilities by 2030. It aims to enhance public services, improve operational performance, and support national security through innovative and resilient digital solutions.

2.4 Home Office Digital supports the Home Office Digital Strategy by ensuring that:

2.4.1 the data the department holds is used effectively and appropriately.

2.4.2 the opportunities for insight gained from this data are maximised, underpinning transformation within operational business areas; and

2.4.3 there is a single point of accountability for all matters relating to IT.

Crown Commercial Service


2.5 The strategy is built around eight strategic shifts (as outlined in the diagram above), including the adoption of AI and automation, investment in modern, maintainable systems, and the creation of a more agile and secure digital infrastructure. It also prioritises improved data sharing, a reimagined digital operating model, and the development of digital skills across the workforce.

2.6 Recent digital improvements—such as streamlined passport renewals, digital immigration status checks, and faster border crossings—highlight the department's commitment to user-focused, scalable services. The 2030 strategy seeks to build on these successes to ensure services remain responsive, efficient, and future-ready. Security is also a central pillar, with a strong emphasis on cyber resilience and the protection of sensitive data.

2.7 Within Home Office Digital the Migration and Borders Technology Portfolio (MBTP) encompasses all technology delivery in four key product areas: Immigration Case working, Border Systems, Passports and Civil Registration, and Platforms.

2.8 MBTP is organised in a product-centric way, with business requirements met where possible by leveraging a set of strategic technology products.

2.9 MBTP Platforms is responsible for supporting Migration & Borders systems resilience through consolidated and streamlined operations across all the products. These products underpin critical national infrastructure and are fundamental components in keeping our borders open, and in managing asylum and visa processing. Any downtime can result in queues at ports, visas and asylum cases being unprocessed, backlogs being created, and revenue lost.

2.10 The CtB (Crossing the Border) product family within includes Border Applications such as Border Crossing (BX), Helios, eGates, Data Platforms, Atlas Platform, platform integration services and hosting platforms.

Crown Commercial Service

## 3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 The Requirements section details the scope of activities to be conducted by the Supplier and the role they will play. This section is intended to give a broad and general overview of the Service Requirements contained within this document and should not be taken as exclusive or limiting. The requirements outlined in the Requirements section take precedence over the Summary of Requirements.

3.2 Crossing the Border (CtB) is the steady state services and products which control the flow of people and services across the UK border. This is done principally via the Primary Control Points, mediated by a Border Force officer, or via an e-gate indirectly supervised by Border Force officer/s. Information from ports is processed by a central collection of systems, hosted in the cloud and on premise. These systems are built on top of a number of infrastructure platforms, leveraging a hybrid cloud model.

3.3 Border Platforms is a hybrid cloud hosting service that sits within MBTP Platforms and is responsible for building and maintaining the hybrid platform which enables tenant teams (currently Crossing the Border) to effectively develop and run current and future services that keep the UK border operational. Border Platform acts as the primary interface to the underlying infrastructure - EBSA for Official (O) and HODC for Secret (S) supporting applications, as well as associated services. It encompasses a broad scope, including the design, build, and maintenance of platform-level products and services that CtB Application teams rely on to develop and operate current and future capabilities.

## 4. DEFINITIONS

| Expression or Acronym | Definition |
|---|---|
| Approval to Operate | means a process of Certification and Accreditation so an IT system can be granted an Authority to Operate (ATO) by the Home Office |
| Availability Management Process | means the process of ensuring the agreed levels of service availability are achieved and maintained in line with relevant Buyer strategy. |
| Border Platforms | means the O and S platforms used to host the products within the CtB Product Family |
| Border Force | means the Buyer directorate responsible for control of the UK border |
| Buyer | means the Home Office |
| Buyer Data | means any documentation, information or data provided by the Home Office or accessed by any third-party provider to enable the delivery of the Services |
| BX | means the Border Crossing (BX) product which is made of several parts - Passenger Control Point (PCP) allows Border Force officers to search passenger records using biometrics and documents. BX Tools allows Border Force officers to investigate passengers more |

| | |
|---|---|
| | thoroughly, either before, during or after they have crossed the border. BX admin tool provides authorised users with access to BX audit and performance data. |
| CCS Technology Services 3 Framework | means the Crown Commercial Service Technology Services 3 framework agreement RM6100 |
| CIS | means critical security control measures in place to help identify, manage and mitigate cyber security threat |
| CMDB | means configuration management database |
| Commencement Date | means the date specified as such in the Order Form |
| Components | means the individual parts of a service or application |
| Configuration Items | means a fundamental unit of a configuration management system that has distinct requirements, functionality and/or product relationships |
| Contract | means the contract between the Supplier and the Buyer for the delivery of the Services |
| Contract Term | means the term of the contract awarded as a result of this procurement, in this instance 4 years plus an optional 1-year extension |
| CtB | means Crossing the Border |
| CtB Product Family | means all the digital services and programmes associated with the Borders and Migration Portfolio which include but not limited to BX, Helios, FBIS, MBTP, ATLAS, Core Cloud, Border Vision, ETA's, E Visas and EBSA |
| Customer Data | means any documentation, information or data provided by the Home Office or generated, processed, stored or transmitted by any third party provider which must be handled in line with the Data Protection Act 2018 |
| Cyber Security Operations Centre | means the systems and processes in place to monitor the health of cyber space and co-ordinate incident response |
| DDaT (now known as Home Office Digital) | means the Digital, Data and Technology directorate provides the Authorities internal and external facing IT and digital services. The function is now known as Home Office Digital |
| DDOS | means distributed denial of service |
| DevOps | means the software development methodology that combines and automates the work of software development (Dev) and IT operations (Ops) teams to accelerate the delivery of higher-quality applications and services |
| Discovery Phase | means the period following contract award where the Preferred Provider will complete a deep dive to establish the detail required for transition of Services and develop the final service deliver plan |
| DV | means developed vetting check as detailed at National security vetting: clearance levels - GOV.UK (www.gov.uk) |
| End User | Means consumers of the CtB business applications |

| | |
|---|---|
| EBSA | Environment Build Support Administration - means the authorities hosting platform build on AWS where CtB O-side applications are hosted |
| Facility Security Clearance | means the measures in place to ensure the Preferred Provider meets and maintains the required protective security controls to safeguard classified assets. It provides the Buyer with assurance that these assets will be appropriately protected. |
| FBIS | means Future Borders and Immigration Systems, the UK's digital products and services used for management of immigration services |
| FinOps | means a framework and set of best practices to manage, optimise and gain financial accountability for cloud spending. |
| Government Secure Intranet | means the intranet used by the government for classified information |
| Government Security Classification Marking | means the security marking used to classify the sensitivity of information and the security measures to be used when handling such information as detailed at Government Security Classifications - GOV.UK (www.gov.uk) |
| Helios | Helios means the system used for the ingest, maintenance and sharing of watchlist data. This data then supports the end-to-end passenger journey - from visa applications and pre-departure checks right through to crossing the border. |
| HMG Security Policy Framework | means the framework which sets out the expectation of how Government organisations and third parties handling Government information and other assets will apply protective security to ensure effective, efficient and secure working as detailed at Security policy framework - GOV.UK (www.gov.uk) |
| HMPO | means HM Passport Office |
| HPI | High Priority Incident - means a Service Incident which is of Priority 1 (P1) or Priority 2 (P2). |
| HODC | Means the Home Office Data Centre |
| IDS/IPS | means Intrusion Detection Systems and Intrusion Prevention Systems which are both means of network security. IDS is a network traffic monitoring solution. IPS is a preventative solution, which blocks delivery of certain documents/information, acting in a similar way to a firewall. |
| Impex | means import and export |
| Implementation Period | Means the Interim Mode of Operation period as defined in Attachment 2 (Charges and Invoicing) and as detailed in the Transition |

| | |
|---|---|
| | Plan in Attachment 3 (Outline Implementation Plan) and which will precede BAU Service Delivery. |
| IPT | means Immigration Platform Technology |
| ITIL | means Information Technology Infrastructure Library |
| JIRA | means the project management software which is used to manage projects and track bugs. |
| KPI | means Key Performance Indicator. KPI's are used as measurable performance metrics which will allow the Buyer to track and manage performance against these set metrics. |
| Level 2 Support | means IT technical Support to provide assistance on issues that level 1 support has been unable to resolve. Level 2 support involves in-depth troubleshooting, technical, and backend analysis |
| Level 3 Support | means IT technical Support that Level 2 is unable to resolve. It is the highest level of IT technical support. Providing in depth examination of incidents and issues. |
| MBTP | means the Home Office Migration and Borders Technology Portfolio Directorate who deliver digital and technology services for the protection of the UK border |
| National Cyber Security Centre | means the UK government agency that provides cyber security advice, guidance and support to industry and the public |
| National Security Vetting | means the security checks required to provide services to government as details at National security vetting: clearance levels - GOV.UK (www.gov.uk) |
| O Side | means the cloud based platform and applications used to hold data marked as Official |
| Parties | means the Buyer and the Supplier |
| PKI Certificates | means Public Key Infrastructure (PKI) certificates are electronic documents that are used to prove the validity of a public key. They include information about the public key, the identity of the owner, and are digitally signed by a trusted entity. |
| PNR Data | means passenger name record (PNR) data, information collected by airlines and other passenger service operators as part of their normal course of business and includes information required to complete and process a booking |

| | |
|---|---|
| Preferred Provider | means the Supplier with the highest total average score after evaluation of Supplier technical and price bids; |
| Product Family | means all the digital services associated with the Borders and Migration Portfolio which include but not limited to BX, Helios, FBIS, MBTP, ATLAS, , Border Vision, ETA's, E Visas and EBSA |
| Border Platform Users | Border Platform users are CtB product teams including DevOps Engineers, Business Analysts, etc who uses the platform services to build and integrate CtB applications hosted on EBSA (Official) and HODC (Secret) environments. |
| RACI | means the document for identifying key stakeholders and their responsibility or level of activity in relation to a project or programme of works |
| RAID | means Risk, Assumptions, Issues and Dependencies log |
| RPO/RTO | means recovery point objective and recovery time objective |
| Secure by Design Principles | means principles developed by the Central Digital Data Office to drive outcomes and their adoption is mandatory across central government and ALBs. They promote consistent and coherent security ways of working in digital delivery. Organisations which already have a local Secure by Design approach - or elements of one - will be expected to adhere to the principles, although they may wish to develop additional ones (and activities) to cater for their own circumstances. |
| Security Check or SC | means the security clearance level for individuals with access to information classified as OFFICIAL SENSITIVE |
| Service Acceptance and Assurance | means the service acceptance criteria used to meet service requirements including functionality, operational support, performance, security to meet functional/non-functional requirements. These activities are undertaken to ensure new releases can be properly supported as part of the Live Service |
| ServiceNow | means the Buyer's Service Management toolset, used for IT incident management, problem management, change management, risk management, knowledge management, asset management and IT requests |
| SIEM | means security, information and event management |
| SLA | means service level agreement, the service levels to be met by the Preferred Provider to deliver the Services to the required standards |
| S Side | means the Buyer platform and applications used to hold data marked as Official Sensitive and above |

| | |
|---|---|
| Supplier | means a company or other entity that submits a Tender in response to the Further Competition Invitation |
| SWG | means Security working group |
| SyOps | means systems operation and IT operations management |
| The Services | means the services outlined in this Attachment 3 Service Requirements document |
| UK EYES ONLY | means the security classification applied to information and data of a level of sensitivity that cannot be viewed by any individual that is not a UK national |
| VPN | means virtual private network |
| WAF | means web application firewall |
| Working Day | means any day other than a Saturday, Sunday or public holiday in England and Wales. |

## 5. SCOPE OF REQUIREMENT

5.1 The Buyer requires Supplier the supplier to provide services to run, maintain, manage, and develop, as needed both the O* platform provided by AWS and the S* secure platform hosted by the Buyer.

5.2 The Supplier will work collaboratively with the Buyer to provide following key services:

5.2.1 Maintain and sustain existing CtB platforms and the current service
5.2.2 Work collaboratively and transparently to deliver all prioritised backlog items including Technical Debts in a cost-efficient way
5.2.3 Drive innovation to improve user experience
5.2.4 Assist the Buyer in implementing key strategies to support the Services

5.3 The following requirements are especially relevant to meeting Border Platform's ways of working needs:

5.3.1 The Supplier shall ensure that all services delivered under this contract are fully aligned with the latest Home Office Digital Strategy.
5.3.2 Be agile at scale

5.3.3 Have consistency of delivery tooling across all teams to enable team based and full roadmap views of the work undertaken. Transparency of this to the Buyer will be provided upon request
5.3.4 Manage demand for roadmap outcomes, including velocity and capacity planning
5.3.5 Collate backlog items per team for consideration and prioritisation as part of the CtB PI Planning to feed into quarterly Roadmap baselining.
5.3.6 Take an active role in quarterly baselining for team roadmaps that feed into an overall Roadmap for CtB delivery, that will be used to inform the forward schedule of Change published and shared with stakeholders.
5.3.7 Manage competing priorities and new requests presented via the CtB Demand Management process and governance meetings.
5.3.8 Enforce RAID management across teams and manage both internal and external dependencies with rigour, ensuring full documentation and evidence of agreement to dependencies.
5.3.9 Ensure robust Risk Management across all Delivery and Service risks- linking these to operational and security risks where appropriate.
5.3.10 Using CtB Risk management process, ensure Risks and Dependencies are documented, reported on in fortnightly progress reviews and are escalated when blocked
5.3.11 Be available for changes and releases which need to be conducted outside CtB Tenant working hours or at weekends. Some out of hour's work will be required
5.3.12 Ensure delivery reporting is included in the Contract Management monthly reports during the Contract Term
5.3.13 The Supplier will provide Platform User Support by communicating effectively with CtB and other relevant stakeholders using Home Office tools such as Slack, Microsoft Teams, and Atlassian tooling, specifically Confluence, and Jira
5.3.14 The Supplier must provide the Buyer with appropriate information to measure the performance of the Service against the agreed KPIs and measures in line with Service Integrator monitoring and governance processes developed during discovery and mobilisation.
5.3.15 The Supplier shall ensure that the service has appropriately skilled resources to effectively deliver the Services.
5.3.16 The Supplier shall work with the Buyer to understand priorities and changes to the Service
5.3.17 The Supplier shall monitor and report on the Service Availability and Return to Service statistics on a Monthly basis including reporting Root Cause Analysis (RCA) progress.
5.3.18 The Supplier shall take ownership and management of Platform and delivery risks including mitigation plans, target dates, and owners for approval by CtB.
5.3.19 The Supplier shall ensure consistency of tooling across its teams for workflow and Delivery Management. This will permit team-based and full roadmap views of work being planned and delivered, which can be manipulated to show multiple views of the same information according to demand. (The Buyer is currently using Jira advanced Roadmap).
5.3.20 The supplier shall, in collaboration with the Buyer, Service integrator and other ecosystem suppliers develop and adhere to a CtB governance structure to ensure delivery across the whole of the ecosystem is aligned.

5.4 A description of each, in scope product or service that is managed across the Border Crossing and Helios teams can be found in Annex 5:

## 6. THE REQUIREMENT

6.1 The Supplier will be required to complete a Discovery and Mobilisation Period during which they will work with the Buyer, incumbent suppliers, Buyer Home Office Digital stakeholders and any other stakeholders, as deemed necessary, to develop a detailed roadmap and delivery plan, including service levels and acceptance criteria which will be agreed with the Buyer and Service Integrator informing the entire ecosystem.

6.2 Border Platforms is made up of sub-products that provide services to CtB. Sub-products are categorised in line with the service provided, and we expect the sub-products and categories to increase in line with demand, and requirement for new capabilities.

6.3 Border Platforms objective is to provide a stable and resilient, highly reliable, and highly available platform, with a route to production, over the S* and O* side infrastructure, for our tenant teams.

6.4 Border Platforms works closely with internal and external, third-party infrastructure providers to ensure services are operating to the highest degree of availability and provide tenants with a resilient service. This includes building and maintaining components that enable secure data sharing between S* and O*, as well as building capabilities to other platforms.

6.5 Service Management Requirements: Home Office Service management requirements are guided by frameworks such as ITIL (Information Technology Infrastructure Library), which provides best practices for managing IT services.

6.6 The Supplier must ensure all Infrastructure services are subject to regular configuration audits Frequency of audits will be agreed following discovery and mobilisation but no less than Quarterly

6.7 The Supplier must maintain a comprehensive, accessible service catalogue.

6.8 The Supplier must perform Root Cause Analysis (RCA) for all high-priority incidents.

6.9 The Supplier must support monthly service reviews including KPIs, trends, and forward planning.

6.10 The Supplier will work in collaboration with the Buyer, System Integrator, the Buyer Service Desk, users, stakeholders and Buyer's other 3rd Party Suppliers providing IT services.

6.11 The Supplier will ensure confidentiality, integrity and availability of data taken from the Supplier ServiceNow system either manually or via an interface.

6.12 The Supplier must identify Incidents to be Resolved either by the User or Service Desk as First Contact Resolution (FCR) and provide all supporting up to date information to enable this.

6.13 The Supplier will use the Buyer's ServiceNow system for the following IT Service Management Processes:

6.20.1 Incident Management

6.13.1 Problem Management

6.13.2 Change & Release Management

6.13.3 Service Request Fulfilment

6.13.4 Certificate Management

6.13.5 Service Mapping

6.13.6 Risk Management

6.14 The Supplier will use the Buyer's ServiceNow as the master record for Incident Resolution Service Levels.

6.15 The Supplier will propose a method for automatically open/close support Tickets within ServiceNow or any successors. To be validated and agreed with the Buyer.

6.16 The Supplier monitoring solution will provide information to the Supplier, data feeds to the Buyer's IT Operations Centre (ITOC), and a feed of filtered Event data to End Users ServiceNow tooling in real time.

6.17 The Supplier's monitoring solution will provide end-to-end measurements of performance across the Services.

6.18 The Supplier will utilise the Buyer's Monitoring and Alerting Tooling. However, the Buyer will be responsible for defining the Monitoring and Alerting thresholds within the tooling. The Supplier must ensure that all Events generated from the Monitoring and Alerting tooling raise a Service Incident within ServiceNow.

6.19 The Supplier must comply with the Buyer's ways of working and standards for ServiceNow tooling.

6.20 The Supplier must conduct Load Testing, ensuring that the solution is able to run a comprehensive performance test suite against the Services so that the Buyer can measure the performance of the Services before promoting it to the live environment. Where applicable, the Supplier must ensure that any fixes are able to run a comprehensive performance test suite against the Services, so that the Buyer can measure performance before promoting it to the live environment.

6.21 The Supplier must make available to the Buyer for review or audit purposes the Supplier's operational processes.

6.20.2 The scope of the Border Platform Support Services is:

6.20.3 Service Hours Monday to Friday excluding Bank Holidays - 08:00 to 17:00 hours.

6.20.4 On-Call Support service 24 hours x 7x 365 days service - Out of Hours On- Call Support service operates from 17:01 hours until 07.59 hours Monday to Friday, all day Saturday and Sunday including Bank Holiday for P1 and P2 Incidents for both O side and S Side.

6.20.5 The Supplier shall provide on site support within 30 minutes, with access to a secure room 24/7 365 to support incident management and associated processes for S components. The access to the secured room will also be required for business as usual tasks and releases

6.20.6 Changes to the Production Environment are expected to take place at any time during the hours of service as agreed with the Buyer. Outside of standard working hours

changes will be conducted following agreement between the Buyer and the Supplier

6.22 **Definitions of Incident Priority**

**The incident descriptions, response and resolution times below will be used defining and prioritising incidents**

| Priority | Description | Response Target | Resolution Target |
|---|---|---|---|
| P1 | P1 means an Incident:<br><br>a) that results in a complete or substantial loss of the Service; or<br><br>(b) that results in an essential part of the Service being unusable for all End Users; or<br><br>(c) that results in all End Users being unable to access the Service. | 100% <= 15 mins | 100% <= 4 hours |
| P2 | P2 means an Incident:<br><br>(a) where the Service is materially adversely affected, but can be circumvented; or | 100% <= 30 mins | 100% <= 8 hours |

| | | | |
|---|---|---|---|
| | (b) where the Service remains operable, but certain material aspects of the Service are disabled; or<br><br>(c) where a large group of End Users is unable to access the Service; or certain material aspects of the Service. | | |
| P3 | P3 means an Incident:<br><br>(a) that results in a minimal business impact for the Service where non-critical functions or procedures are down, unusable, or difficult to use; or<br><br>(b) affecting a single or small group of End Users. | 100% <= 24 hours | 95% <= 2 Working Days<br><br>100% <= 5 Working Days |
| P4 | P4 means an Incident: | 100% <= 48 hours | 95% <= 3 working days |

Crown Commercial Service

| | | | |
|---|---|---|---|
| | (a) that results in little or no material impact on the Service or the Customer's business; or | | 100% < 5 working days |
| | (b) where the Service is determined to be functioning as designed but the Incident may result in a Change Request to modify or enhance the Service; or | | |
| | (c) raised in response to questions, compliments, complaints, escalations, or queries from the Customer. | | |

6.23 **The Buyer also uses a standardised internal incident definition which the suppliers maybe asked to conform to but will not be measured against which is below.**

| **Priority** | **Description** |
|---|---|
| P1 | An incident that causes major disruption to Home Office services with an immediate impact on public safety, national security, essential citizen-facing operations, corporate functions, compromised or the loss of personal data or the risk of reputational or financial damage.<br><br>In previous similar incidents, it warranted urgent, around-the-clock response to restore services. |

| | |
|---|---|
| P2 | An incident that has a direct, but non-critical impact on Home Office services, which if left for more than up to 8 hours would impact on public safety, national security, essential citizen-facing operations, corporate functions, compromised or the loss of personal or sensitive data or the risk of reputational or financial damage.<br><br>The goal is to avoid the incident escalating to a P1.<br><br>Important to note that the recovery approach will match P1 as there are SLA's and Supplier agreements where resources are not committed unless a P1 is declared. |
| P3 | An incident that impacts Home Office teams and operations but has no direct impact on public safety, national security, essential citizen-facing operations, corporate functions, or the risk of reputational or financial damage. |
| P4 | An incident that impacts individuals or parts of teams but has no direct impact on Home Office operations, public safety, national security, citizen-facing services, corporate functions, or the risk of reputational or financial damage. |

6.24 The Supplier must work with the Buyer to agree and prioritise Incidents should conflict occur during On-Call Support.

6.25 The Supplier shall support all Incidents raised against Operations, Production and Non-Production (excluding development) Environments of the Services

6.26 The Supplier must provide an On-Call Support rota for those services covered by this contract.

6.27 The Supplier must collaborate with the Buyer to produce a rolling schedule and implement Continual Service Improvements (CSI) against prioritised Backlogged technical and service improvement requirements.

6.28 The Supplier shall use Continual Service Improvement (CSI) methods to improve quality, reduce failures and implement lessons learned with objectives measured in the following key areas:

6.27.1 Service efficiency savings

6.27.2 Service Level improvements

6.27.3 Automation

6.27.4 Service agility

6.27.5 Service improvements.

6.29 The Supplier shall identify areas for continuous improvement of the Services process, and demonstrate proactive steps to drive cost savings, process efficiency and service quality. To be agreed during discovery, at least quarterly.

6.30 The Supplier must ensure adequate capacity planning is implemented, including but not limited to:

6.29.1 Determining required infrastructure resources and capacity

6.29.2 Calculating current capacity and determine any gaps

6.29.3 Aligning capacity with demand

6.31 The Supplier must mitigate service impacts by pre-empting performance issues through monitoring capacity and recommending required action to the relevant party, as agreed with the Buyer.

6.32 The Supplier must monitor certificates and notify the Buyer at least 3 months in advance of certificate expiry dates

6.33 The Supplier shall record, maintain and organise an inventory of certificates, including costs and expiry dates using the Certificate Inventory for the Buyer or any replacement system.

6.34 The Supplier shall continually update and monitor certificate inventories, using the Certificate Inventory Dashboard or any replacement system.

6.35 The Supplier shall seek to continually improve the Certificate Management process set out in the Home Office Certificate Management Policy, in collaboration with Buyer teams and the Service Integrator, through process and technical improvements

6.36 The Supplier must deliver improvements plans, which will be set and assured by the Buyer

6.37 The Supplier shall comply with the Buyer's Certificate Management standards, including National Cyber Security Centre (NCSC) published guidelines

6.38 The Supplier shall be responsible for Infrastructure Certificate Management related to Infrastructure, Networks and security. Some Certificate Management will be automatic and owned by Buyer teams, and not in the remit of the Supplier.

6.39 The Supplier shall introduce an escalation process to ensure the decision makers are informed of certificate issues relevant to their function, integrated into ServiceNow.

6.40 The Supplier shall ensure all non-service impacting Changes required for ongoing maintenance are standardised, pre-approved and automated unless otherwise agreed with the Buyer.

6.41 The Supplier shall adhere to the Buyer's Release Management Home Office Operating Model for Change Enablement.

6.42 The Supplier shall comply to the principles and policies as defined in the Buyer Home Office Operating Model for Change Enablement, in their support and maintenance role.

6.43 The Supplier shall provide and manage impacting and non-impacting standard Changes, normal Changes and a forward schedule of Changes according to the processes described in the Buyer Home Office Operating Model for Change Enablement

6.44 The Supplier shall make Emergency Changes as required to Resolve or prevent a P1/P2 Incident or to address a security issue, as required and within the Buyer Home Office Operating Model for Change Enablement, in accordance with SL2.

6.45 The Supplier must take ownership of all Changes, Problems and Incidents that relate to in-scope Infrastructure service components.

6.46 The Supplier shall conduct scheduled and non-scheduled maintenance tasks to Platform, requiring patching, covering code, operating systems, and other products in consultation with relevant stakeholders (emergency patches, planned patches/upgrades, third party dependencies, i.e. new versions of COTS products).

6.47 The Supplier shall conduct development, Testing, communication to stakeholders and packaging of changes and upgrade in readiness for Release deployment of scheduled and non-scheduled maintenance.

6.48 The Supplier shall provide code and configuration management.

6.49 The Supplier shall participate in the Buyer's change management processes.

6.50 The Supplier shall engage the appropriate technical teams to provide an impact assessment of the Changes.

6.51 The Supplier shall in a timely manner work collaboratively with the Buyer Test and Tenant Delivery Teams to coordinate and plan release and agree dependencies across the platform for application testing environments and the route to production.

6.52 The Supplier must create TIPs (Technical Implementation Plan), which are impacted assessed, reviewed, include risk and 'blast radius' views, rollback plans, pre and post deployment checks, to be tested prior to go live and re-confirmed in production.

6.53 The Supplier will be required to work with Buyer, HO Digital and ensure compliance with the Authorities release strategy to ensure planned releases and maintenance do not affect overall system availability.

6.52 The Supplier shall maintain critical services as listed below.

6.52.1 Enhance and maintain the platform to enable tenant teams to effectively develop and run current and future services that keep the UK border operational.

6.52.2 Produce, and manage the delivery roadmap, driven by the Buyer owned product roadmap, which is to be aligned with tenant & MBTP Platforms environments. This includes aligning processes and governance to minimise duplication, and inconsistencies further streamlining and making efficient the services provided.

6.52.3 Identify and implement efficiencies making process and delivery leaner, including use of new technology to drive innovation.

6.52.4 Provide products, including appropriate proactive monitoring and maintenance, to attain a minimum of 99.93% availability of the production environment.

6.52.5 Continuously improve the platform, processes, and delivery methods of products to enhance the live service, drive value for money and efficiency

6.53 Increase and maintain resilience and availability of critical services.

6.53.1 The Supplier will manage and support critical national infrastructure, with appropriate onshore facilities, providing 24X7x365 monitoring and ability to facilitate immediate responses to incidents.

6.53.2 The Supplier will ensure all services are developed and maintained in line with MBPT security standards and Secure by Design (SbD) principles.

6.53.3 The Supplier will manage and maintain the non-production environments to ensure all issues are resolved promptly and environments made available.

6.54 The Supplier will be required to work with the HO Digital Change & Release Management Teams to raise changes, impact assess and validate changes being implemented by other product/ delivery teams.

6.55 The Supplier will be responsible for increasing resilience of the platform, working closely with infrastructure providers and CtB Applications to minimise service interruption.

6.56 The Supplier will increase availability of services through non-impacting releases.

6.57 The Supplier will reduce impacting releases and keep downtime of core services to a minimum NFR's for CtB Products. NFRs for other products and services will vary and should be adhered to.

6.58 The Supplier will enhance monitoring and alerting capabilities (including integrations)

6.59 The Supplier will increase automation (e.g. pipeline builds)

6.60 The Supplier will improve the engineering posture ensuring sustainability of products and services.

6.61 The Supplier will increase test coverage to ensure all components are incorporated into the products test strategy.

6.62 The Supplier will be data driven, inspect & adapt by making use of available data to drive high quality delivery through data driven decision making.

6.63 Enable users to easily deploy and maintain applications;

6.63.1 The Supplier will work in partnership with all stakeholders in Home Office Digital and its partners in an atmosphere of openness and transparency. Home Office Digital expects all stakeholders, partners, and suppliers to work collaboratively, transparently and in partnership to successfully achieve its outcomes

6.63.2 The Supplier will measure and improve CtB Platform user satisfaction through regular surveys and feedback analysis. Supplier will provide reports summarising score, trends and actions taken must be presented at CtB governance meetings. Frequency of reports will be agreed during Discovery and Mobilisation.

6.63.3 The Supplier will improve tenants' ability to self-serve (e.g., pipelines, running tests locally, tooling etc.)

6.63.4 The Supplier will increase availability of test environments

6.63.5 The Supplier will streamline release process, enabling more to be delivered quicker.

6.64 Product Catalogue - The Suppler shall monitor, add and maintain the Buyer Product Catalogue. The Supplier must ensure that introduction of new Product Catalogue items will not create any Platform infrastructure performance issues.

6.65 The Supplier will provide L3 support

6.66 Border Platforms is made up of products that provide services to CtB. The products are categorised in-line with the services they provide. We expect the product categories to grow in-line with demand and requirements for new capabilities.

6.67 The products and services are grouped into five categories, as follows;

Crown Commercial Service

6.68 Platform Tools are a collection of tools and frameworks to facilitate the development of the applications or services that are hosted on the platform. These components expose the core foundational capabilities to the application team developers.

6.69 Platform Foundational Capabilities are standard components that make up the foundations of the platform that are utilised by the applications.

6.70 Production and release support covers support activities, management of dependencies with infrastructure providers, management of platform applications and S* side deployments.

6.71 The Supplier will provide 2 distinct types of support, non-production environment support and Level 3 DevOps support for production.

6.72 Non-production support is the maintenance of non-production environments to ensure smooth functioning, testing and development of software before it reaches production environments.

6.73 Production support is Level 3 on-site and on-call support 24/7 365 across all areas of the platform to address critical issues.

6.74 Production support will require highly skilled technical capabilities 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.

6.75 Level 3 are expected to collaborate with Level 1 and Level 2 as well as other teams (e.g. EBSA, CtB Application, etc) and wider stakeholders as required to ensure the continued availability and high quality of products and services.

6.76 Operational Sustainment: The EBSA Platform currently hosts CtB applications and is based on existing AWS Cloud infrastructure. Core Cloud represents the strategic foundation for the department's future cloud services. Its primary purpose is to enable cross-Home Office delivery by integrating tools, processes, automation capabilities, and technologies, allowing development teams to deliver products faster and more efficiently.

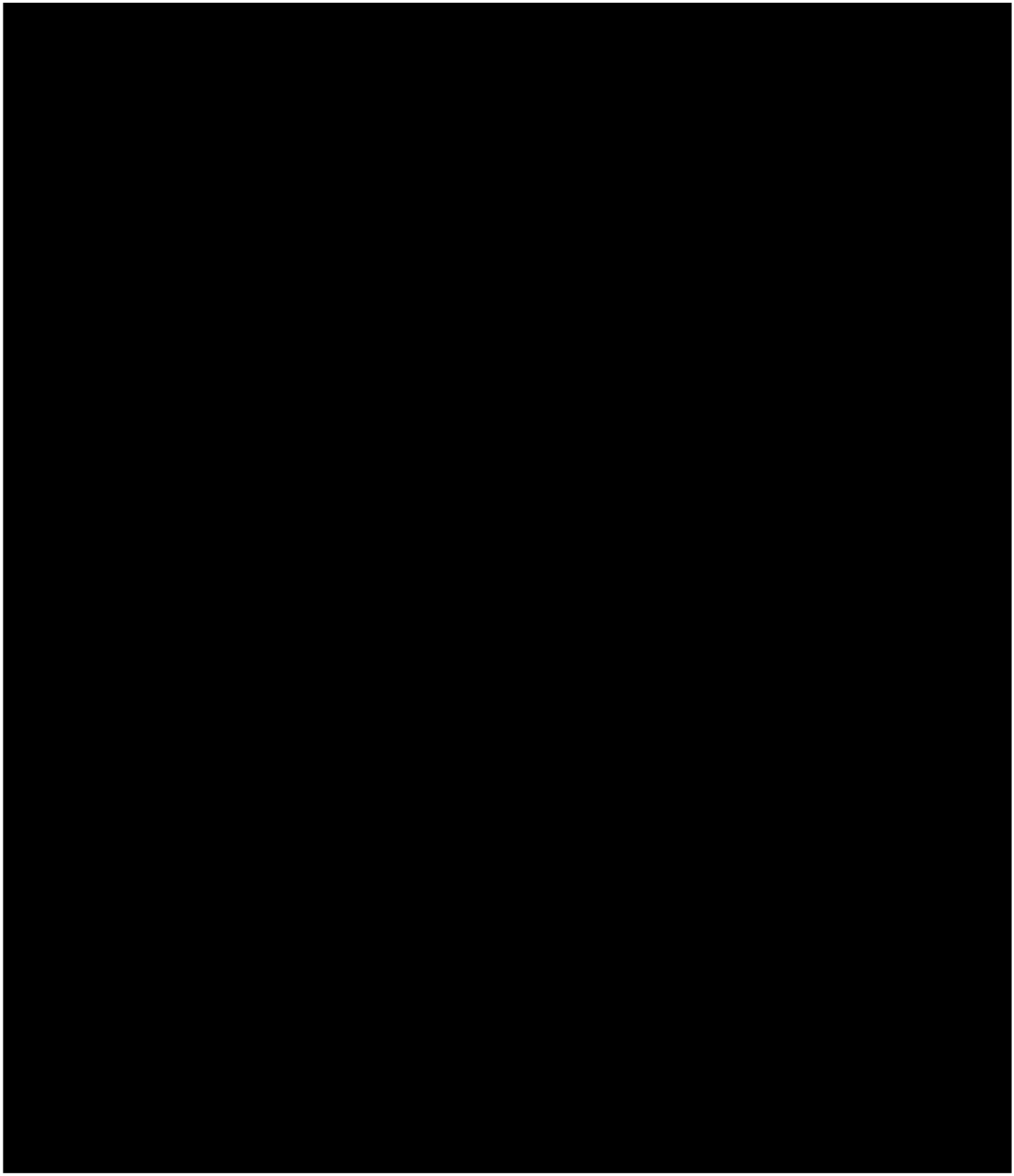
6.76.1 Work will be required on the CtB Platform to enable CtB applications to transition to Core Cloud. This involves safely migrating services from the EBSA Platform while maintaining uninterrupted service. The Core Cloud strategy and migration will be prioritised by the Home Office at an appropriate time.

6.76.2 While the strategic direction for Home Office Digital platforms is to adopt Core Cloud, it is recognised that the CtB EBSA Platform presents specific risks that must be addressed in the interim. These mitigations will serve as a stepping stone to enable the safe transition of platforms and applications to Core Cloud.

6.77 The supplier will manage the relationship between CtB tenants and infrastructure providers (e.g. EBSA) so that the application tenants get a consistent infrastructure experience regardless of the platform.

6.78 **S side support.** The Supplier shall provide onsite support within 30 minutes for all P1 and P2 incidents, with access to a secure room 24/7 365 to support incident management and associated processes. The access to the secured room will also be required for business-as-usual tasks and releases as outlined in the requirements.

Crown
Commercial
Service



Crown
Commercial
Service

## 7 TECHNICAL DEBT

7.1 The Buyer Technical Debt is:

7.1.1 Technical debt is generated in a number of different ways - from a sub-optimal solution introducing risk and cost to a Product, to the cost of extra work caused by delivering a tactical solution sooner rather than delivering the most effective solution first time around.

7.2 The Supplier will be responsible for identifying, managing, and remediating technical debt in close collaboration with the EBSA, CtB Application teams, architecture, Service Management and other relevant stakeholders.

7.3 Technical debt must be clearly documented, prioritised, and scheduled for remediation as part of the platform's ongoing business-as-usual (BAU) maintenance activities. Additionally, any platform upgrades must incorporate relevant technical debt remediation. All remediation efforts must be updated against the products and formally agreed with the Buyer.

7.4 The Supplier will ensure that technical debt is managed to sustainable levels which includes working closely with the central CtB tech debt management process, ensuring there is clear visibility to the board of any cross-cutting tech debt and dependencies.

7.5 Tech debt will be assessed against other priorities, and scheduled in with minimal disruption to border services

7.6 The Supplier will manage the products and services to ensure all components are maintained to specified levels and supported versions.

7.7 Current Platforms Technical Debt can be found within Annex 1

## 8 KEY MILESTONES AND DELIVERABLES

8.1 Throughout the delivery of the Service, the Supplier is required to take responsibility for business analysis, software development and test activities within the lower environments for the duration of this Contract. All release management and integration test activities are the responsibility of the Buyer with support from the Supplier.

8.2 The Supplier is required to facilitate the operation of a pipeline process, which will be used to determine the scope of work for the project, including both Supplier's and Buyer resources. The process will provide a pipeline of needs from the Buyer, measure these needs against the available delivery capacity, and make decisions about prioritisation. These decisions will determine what functional scope is delivered and when. In the case of conflicting Buyer stakeholder priorities, the Buyer Product Manager has the final say in prioritisation of work by the Supplier.

## 9 MANAGEMENT INFORMATION/REPORTING

9.1 Reporting requirements will be captured in the Governance Schedule under Transparency Reporting, and these will be defined and agreed during discovery and mobilisation period.

9.2 Operational reporting and associated management processes such as RAID etc will be defined and agreed post engrossment.

## 10 VOLUMES

10.1 Volumes will be determined post Discovery phase and during the deep dive phase.

Crown Commercial Service

## 11 CONTINUOUS IMPROVEMENT

11.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

11.2 The Supplier should present new ways of working to the Buyer during monthly Contract review meetings.

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

## 12 SUSTAINABILITY / SOCIAL VALUE

12.1 The Buyer also requires the Supplier to demonstrate their commitment to social value by ensuring that throughout the contract term they have activities and processes in place that will show how they embed workforce health and mental wellbeing into their business as usual activities. This includes how they;

12.1.1 Demonstrate action to support the health and wellbeing, including physical and mental health, in the contract workforce, and;

12.1.2 Influence staff, suppliers, customers and communities through the delivery of the contract to support health and wellbeing, including physical and mental health.

12.2 Procurement Policy Note (PPN) 6/20 – Taking Account of Social Value in the Award of Central Government Contracts. 'Social value should be explicitly evaluated in all central government procurement, where the requirements are related and proportionate to the subject-matter of the contract, rather than just 'considered'.

12.3 PPN 06/20 guidance documents can be found at: https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts .

## 13 QUALITY

13.1 The Supplier will ensure a list of accreditations held are relevant to the scope of the Suppliers solution and are maintained throughout the life of the contract.

## 14 PRICE

14.1 Prices submitted are detailed in Attachment 2.

## 15 STAFF AND CUSTOMER SERVICEF

15.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

15.2 The Supplier staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

15.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

Crown Commercial Service

## 16 SERVICE LEVELS AND PERFORMANCE

16.1 The Buyer will measure the quality of the Supplier's delivery by adherence to the following KPI's: The Buyer will measure the quality of the Supplier's delivery by adherence to the KPI's that will be discussed and agreed during the Discovery and mobilisation phase. The early view of the KPI's that may become applicable is as follows:

| | KPI | POOR | UNSATISFACTORY | IMPROVE | ON TARGET | ABOVE TARGET |
|---|---|---|---|---|---|---|
| 1 | IT Governance – Unauthorised changes per month | | | | 0 | |
| 2 | IT Governance – Failed release working group/Go no go checks per month | | | | 0 | |
| 3 | IT Governance – Failed phase gate reviews per month | | | | 0 | |
| 4 | Performance Management – Critical processes with agreed goals and metrics | 80% | 85% | 90% | 95% | 100% |
| 5 | Performance Management – Defect resolution times | | | | To Target | Quicker than agreed target |
| 6 | Enterprise architecture Workstreams using enterprise architecture services | | | | 100% | |
| 7 | Service Management - % of services with defined SLA | <80% | 80% | 90% | >90% | |
| 8 | Compliance with defined service levels | <90% | 90% | 95% | 100% | |
| 9 | Compliance with existing DORA metrics | <90% | 90% | 95% | 100% | |
| 10 | Delivery of outcomes to agreed quality standards | <90% | 90% | 95% | 100% | |
| 11 | Use of tooling, adherence to WoW, standards | <90% | 90% | 95% | 100% | |
| 12 | Availability of requirement information through agreed tooling | <90% | 90% | 95% | 100% | |
| 13 | Supplier leads the understanding and defining of requirements | <90% | 90% | 95% | 100% | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | Transparency on SOW activities and ways of working | <90% | 90% | 95% | 100% | |

16.2 The Supplier must adhere to an Incentives Mechanism and Service Credit regime which will be in force until the end of the contract. The process will be further defined during the Discovery and Mobilisation Period.

16.3 A performance management strategy will be developed during the first 6 months, in collaboration with the Buyer and Service integrator, after contract commencement which will include processes for management of poor performance.

## 17 INICIDENT MANAGEMENT, PROBLEM MANANGEMENT AND AVAILABILITY.

17.1 The Supplier will provide their services as a Level 3 support capability in accordance with the Buyer Home Office Digital's incident management processes.

17.2 These issues will be triaged and resolved by Level 2 Support teams, based on work instructions for common issues or alerts.

17.3 If Level 2 are unable to resolve an incident because it would require a change in the source code or a change in the way the product functions, data errors, or a work instruction is not available; the incident will be raised to the Level 3 support team to provide a workaround. The Supplier will be responsible for;

17.3.1 Root Cause Analysis (RCA) – Provide an impact assessment on the cause of the issue, the impact to end users and recommendations on the resolving the issue

17.3.2 Code Change – If an incident requires a code change, the product team will be responsible for making the change and ensuring it goes through the standard engineering processes.

17.3.3 Design Changes – If an incident highlights an issue in the original design, the architecture team will need to make a design decision on any changes that needs to be made to the design.

17.3.4 Data Corrections – if Data needs to be patched then the Supplier team is responsible for identifying the changes needed and seeking the test evidence and approvals to run these data corrections in Production if they have access or raising a ticket with the appropriate team to run more large scale / complex data corrections.

17.3.5 Work Instructions – If the problem is one that may reoccur in the future a work instruction for Level 2 should be drafted and a knowledge transfer exercise completed to allow Level 2 to resolve these in future without Level 3 input in line with shift left principles.

17.3.8 Collaborating with other teams on incident management Facilitating the restoration of normal service operationAs part of their Level 3 support and development activities or in their regular monitoring of the system, the Supplier is responsible for raising any issues they see in Production with the Level 2 Support teams so appropriate triage and incident management processes can start. Incident Management (L3)

17.5 The Supplier must follow the Buyer's processes and coordinate Platform Incident response and communications with the Buyer

17.6 The Supplier shall conduct diagnosis and remediation of Incidents passed on to Border Platform Service support, related to technical issues or failure of specific infrastructure components, routines, bespoke applications or interfaces (where Buyer Level 2 team have been unable to identify a resolution).

17.7 The Supplier shall build, test (including regression) and package infrastructure solutions to fix the issue identified as part of the Incident and coordinate releases through live services control processes.

17.8 The Supplier must Resolve security related incidents where a core vulnerability is identified requiring Border Platform support intervention in accordance with Cyber Security incident resolution SLA's.

17.9 The Supplier shall provide Workarounds and Resolutions to restore Border Platform.

17.10 The Supplier at the request of the Buyer may request Supplier Staff to participate in Major Incident Management. In these instances, the Supplier team shall divert from their current work to support the Incident.

17.11 The Supplier must in the event of a P1 during Service Hours provide access to subject matter and technical experts for input and advice on infrastructure configuration, monitoring/alerting, and disaster recovery (DR).

17.12 The Supplier must ensure early alerting and well-defined steps to recover from unhandled exceptions processes are in place to enable the Services are able to recover consistently from unhandled exceptions.

17.13 The Supplier must, liaise with the Buyer's High Priority Incident (HPI) Management Team for all P1 and P2 incidents.

17.14 The Supplier must comply with the Buyer Home Office Operating Model for Incident Management and any updates made to it,

17.15 Problem Management

17.16 The Supplier must comply with the Home Office Operating Model for Problem Management.

17.17 The Supplier shall be responsible for undertaking Incident /event trending and to raise Problems proactively for underlying issues which are repeatedly occurring.

17.18 The Supplier must reduce the level of Incident recurrences to allow both the Buyer and the Supplier to identify, prioritise and remediate known errors, faults and recurring issues. For all fault remedy, the Buyer shall be the final decision maker and set priorities. The Supplier and the Buyer shall work together to manage between Service and Delivery dependent on complexity

17.19 The Supplier shall manage, conduct, and distribute Root Cause Analysis (RCA) reports including an implementation plan for the agreed remediations.

17.20 The Supplier shall provide feedback to the Buyer on the Root Cause Analysis (RCA) process with the aim of informing the Buyer on recommendations to improve remediation responses and end-to-end Resolution targets for the Services.

17.21 The Supplier shall provide Incident or Problem reports for Incidents or Problems Resolved by the Supplier.

17.22 The Supplier shall perform trend analysis on Service Incidents assigned to them to inform service improvements and report back to the Buyer as part of the monthly service review meetings.

17.23 The Supplier must engage in Buyer's Problem Management Process if the Services are frequently failing and causing significant impact to the Buyer's End User services. This shall require input from the Supplier to attend regular meetings and update the Buyer with progress updates as requested by the Buyer for un-diagnosed Problems.

17.26 The Supplier will proactively manage and maintain the CtB Platform Product List as per Annex 5 below to ensure availability expectations are met.

17.27 The Supplier will advise and assist in the definition, documentation, agreement, monitoring, measuring, reporting and review of Service Level Agreements (SLAs).

17.28 There will be a requirement to input into Monthly Service Management review. Other key activities will include ensuring the agreed SLAs are delivered, Triage of allocated tickets, providing updates on incidents and problems on the HO service management tooling.

17.29 The Buyer will measure the quality of the Supplier's delivery by adherence to the KPI's agreed following discovery and mobilisation.

17.30 The Supplier must adhere to an incentives mechanism which will be in force until the end of the contract. The process will be further defined during the contract engrossment period.

17.31 A performance management strategy will be developed during the first 6 months after contract commencement which will include processes for management of poor performance.

## 18 SECURITY AND CONFIDENTIALITY REQUIREMENTS

18.1 The Supplier must ensure that all individuals supporting delivery of the services must hold Baseline Personnel Security Standard clearance as minimum. All individuals deployed in the delivery of the services must hold National Security Vetting at Security Cleared (SC) level as a minimum, there will be a requirement for additional security clearance in relation to S side clearance- NPPV3 for any individuals interacting with police data. Please see United Kingdom Security Vetting - GOV.UK (www.gov.uk/government/organisations/united-kingdom-security-vetting ) for further details.

18.2 Suppliers should be advised that where an individual has held SC vetting but has not been engaged on a contract delivering services to government for 12 months or longer, then regardless of the expiry date of the vetting this vetting will no longer be valid.

18.3 Please note valid SC vetting must be in place prior to start of the services and the Supplier will be responsible for sponsoring all vetting and costs for vetting.

18.4 The Buyer will require all SC vetting for individuals deployed in the delivery of the Services to be transferred to the Buyer for the duration of the Contract Term. Prior to start of the

services the Supplier will be required to complete a security clearance transfer form for each individual with SC vetting to be deployed on the Contract.

18.5 The Supplier must ensure that all data shared or produced in the delivery of the Contract carries the relevant Government Security Classification Marking and is treated in accordance with the Government Security Classification Policy, see Government Security Classifications - GOV.UK( www.gov.uk/publications-security-classifications.) for further details.

18.6 The Supplier must ensure compliance at all times with the requirements of the Government Security Policy framework. Please see Government security - GOV.UK (www.gov.uk/government/publications/security-policy-framework.) for further details.

18.7 The Supplier must ensure that any data produced or shared in the delivery of this Contract is not held Offshore. Where the Supplier has a requirement for data to be stored or accessed Offshore then approval must first be sought from the Buyer.

**19 SECURITY MANAGEMENT**

19.1 The Supplier must seek approval of the use of any 3rd party suppliers from the Buyer and shall ensure appropriate Security Assurance is conducted on any 3rd party suppliers used to provide the service before being provided access to the Buyer ICT services.

19.2 The Supplier shall be ISO/IEC 27001 and Cyber Essential Plus compliant. The Supplier shall ensure that they have active ISO/IEC 27001 certification throughout the duration of the contract for any of their locations used to provide any services in scope of this contract.

19.3 The Supplier shall support the service with SC security cleared staff with caveat of UK EYES ONLY that are skilled and competent and have undergone additional the Buyer's onboarding checks and security briefings before engaging them on design or delivery of services. For avoidance of doubt this means that all staff must be UK nationals, staff with dual nationality will need to be reviewed by the Buyer and approved on a case-by-case basis. Supplier Personnel who are unable to obtain the required security clearances must be prevented from accessing systems, which store, process or are used to manage the Buyer's Data except where agreed with the Buyer's in writing.

19.4 The Supplier shall be subject to pre-employment checks that are compliant with ISO/IEC 27001 and ISO/IEC 27002, the Security Policy Framework, and HMG Personnel Security Controls and shall include the verification of, as a minimum: identity, unspent criminal convictions and right to work.

19.5 The Supplier may choose the method of assessment, but it must conform to Good Industry Standards or National Protective Security Buyer (NPSA) 'Personnel Security Risk Assessment' available at: https://www.cpni.gov.uk/

19.6 The Supplier shall ensure that Supplier Personnel that have the ability to access Customer Data or systems holding Customer Data shall sign SyOps documents that commit them to standard security related requirements, undergo regular training on secure information management principles and also undergo any required Buyer led training. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

19.7 The Supplier shall immediately inform the Buyer if the Supplier's environment is subject to a Cyber Attack during the length of the contract. The Supplier shall also make the Buyer aware of any Cyber Attacks it has experienced within the last year, with full details where appropriate of what information was obtained and what was carried out to mitigate the risk.

19.8 The Supplier shall report any non-compliance with the Buyer's Security Policies and Procedures appropriately.

19.9 The Supplier shall support the Buyer's Protective Monitoring Service by sharing information such as threat intelligence, vulnerabilities and less structured information, such as lessons learned reports, with the Cyber Security Operations Centre for situational awareness and tuning. The Supplier will log all such information by utilising the relevant the Buyer's audit logging and monitoring standards.

19.10 The Supplier shall ensure that any data that they generate is retained legally in compliance with statutory or legal obligations such as the Data Protection Act 2018, so that information assurance standards are understood and adhered to in order to manage risk effectively.

19.11 The Supplier shall comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which the Buyer are signatories (e.g. Government Secure Intranet); so that specific aspects of information assurance are understood and adhered to in order manage risk effectively.

19.12 The Supplier shall ensure that Buyer Information, Buyer Data and Information Assets are transmitted in such a way as to ensure that no unauthorised person has access to them and that information assurance standards are understood and adhered to in order manage risk effectively.

19.13 The Supplier shall ensure that there is an efficient system of reporting, recording and investigating breaches of security, which the Buyer security staff can monitor, in accordance with HMG Security Policy Framework, so that the Buyer is informed of the risks and security incidents so that it can respond.

19.14 The Supplier shall ensure that all systems are operated in such a manner to support the Buyer's compliance with HMG Security Policy Framework located at: https://www.gov.uk/government/publications/security-policy-framework.

19.15 The Supplier shall ensure that all National Cyber Security Centre (NCSC) good practice, guidelines or advisories are followed. Where there is none, relevant best industry practises should be followed.

19.16 The Supplier shall support product teams in their work to maintain all systems and information assets to the appropriate accreditation levels, including scheduled annual IT Health Checks or following any significant changes or incidents and management of outstanding risks agreed as part of service acceptance.

19.17 The Supplier shall ensure that all reasonable steps are taken to minimise security breaches in the physical, procedural or technical domains of any asset under The Supplier control. This shall include encryption of all Buyer Data in transit end-to-end, using methods as proposed by the Supplier and agreed with the Buyer.

19.18 The Supplier shall be required to use the Buyer's Supply Chain Risk Tool, currently Risk Ledger, and comply with requirements and requests as directed by the Buyer's Corporate Security function.

19.19 The Supplier shall maintain a Register of Assurance documents, risk assessments, IT Health Check reports and all other associated security artefacts across all in-scope services in Live Production environments, including renewals and key updates to the agreed tooling.

19.20 The Supplier shall provide support via technical means from agreed UK based locations aligned to security and policy requirements. The Supplier will operate from Facility Security Clearance (FSC) accredited sites. The Supplier will safeguard the Buyer data under the UK Data Protection regime and must be able to state the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks the data will be subject to at all times.

19.21 The Buyer data shall not be subject to offshoring arrangements.

19.22 The Supplier shall gain and maintain the Buyer's Approval to Operate for the combination of sites, infrastructure and processes used to deliver the Services.

19.23 The Supplier shall agree with the Buyer a document setting out security risks relevant to the Services, and the way in which they are addressed, together with an assessment of any remaining risks which may need to be accepted, and clear statements regarding any relevant assumptions and external security dependencies.

19.24 The Supplier shall ensure that Supplier Personnel shall comply with the principle of least privilege and shall only be granted increased IT privileges or access rights only to the extent necessary to carry out their duties. When Supplier Personnel no longer need elevated privileges, The Supplier shall revoke their access rights as soon as possible which shall not exceed one (1) Working Day.

20 **PRODUCT SECURITY - DEVELOPMENT SECURITY**

20.1 The Supplier must ensure application development takes place in a secure development environment which controls changes to source code and the release through a pipeline into development/testing/staging environments prior to being released into live production so as to minimise the risks of unauthorised/untested changes and prevents leaking of production information into the non-productive environments.

20.2 Threat and vulnerability management (TVM) - the Supplier must ensure the system uses up to date and supported versions of products and software, it is regularly screened for new vulnerabilities and configuration errors and security patches from vendors are applied on a regular basis to minimise the risk of known vulnerabilities being exploited. All patching must comply with the Buyer's vulnerability management and patch management policies.

**21 NETWORK SECURITY**

21.1 The network must provide sufficient network separation between application/system components depending on their information classification and exposure with strong and robust controls (to include firewalls, WAF, proxies, VPN, IDS/IPS, DDOS Protection) regulating the information flows across the network boundaries.

21.2 Anti-malware - the system must be protected against malware infection and any anti-malware software must be automatically updated at least daily to ensure it remains effective.

**22 ENCRYPTION** The system should ensure information is encrypted in transit on both internal and external networks, at rest as appropriated for IT classification or their assets classification marking, using approved or currently recommended encryption suites PKI certificates are from trusted sources and private keys are secured and managed.

23 **HARDENING** The Supplier should ensure that devices, operating systems, applications or other technology related components are security hardened in accordance with a minimum of CIS level 1 benchmarks and where appropriate CIS level 2.

**24** **IAM** Currently the Buyer's or National Cyber Security Centre (NCSC) guidelines, or in absence of these a minimum of CIS level users and services must be uniquely identifiable and authenticated by a centrally managed identity store with robust role-based access controls for users, developers and administrators following the principals of least privilege and segregation of duties. All access to production applications must be restricted to only Home Office authorised devices from authorised locations. Administrator access to production environments must be restricted to only Home Office authorised devices/locations and be requested or authorised for timebound durations.

**25** **LOGGING AND MONITORING**Security logging must be enabled to support incident investigations, forensics and provide continuous security monitoring to detect suspicious user, administrator or erroneous network activities. Logs must be made available to the MBTP Splunk platform to provide monitoring of the environment against defined security use cases. Logs data will be identified as part of the secure by design process in collaboration with the MBTP cyber security team.

25.2 The Supplier shall assist the Buyer in identifying gaps in Monitoring & Alerting, suggesting improvements to the current implementation and collaborating with the Buyer on the future requirements.

25.3 The Supplier shall commit to a successful, long-term partnership working in collaboration to achieve Home Office objectives, including the continuous knowledge transfer to Home Office staff.

**26** **BACKUP / RECOVERY**Data must be backed up to allow recovery of information destroyed or corrupted by a malicious user, accidentally or through a system failure to meet the RPO/RTOS for the system.

26.2 The Supplier shall test the ITSCM Plan, RTO and RPO objectives on an annual basis, resolve any issues identified, and inform the Buyer of all risks, threats and findings. Testing will be assured by the Buyer.

26.3 The Supplier shall perform all required activities in the ITSCM Plan in the Event that a Service Continuity Event occurs.

26.4 The Supplier's ITSCM plan shall incorporate all content from the Buyer's IT Service Recovery Plan template.

26.5 The Supplier must conduct a review on the ITSCM plan and provide an update to the Buyer at a minimum annually or otherwise requested by the Buyer.

26.6 The Supplier must conform to the Data Backup and restoration policies, standards, and principles as outlined in the Home Office Backup and Restore Standard. This includes ensuring that all systems and data under their management are appropriately assessed, backed up, tested, and restorable in accordance with the defined requirements for Service Continuity, data integrity, encryption, access control, and compliance with the NCSC's secure Design Principles and the Home Office's retention and disposal policies.

26.7

**27** **RESILIENCE** The system should be resilient to single points of failure.

27.2 The Supplier shall design and implement resilience and failover tests for all platform products

27.3

**28** **GOVERNANCE** The security and information risks must be actively governed with monthly reporting on security KPI to the Buyer SWG in order steer and continuously improve the security of the system. At a minimum this should cover risks, security incidents, vulnerabilities and remediation status, security patching, system upgrades and new capabilities.

**29** **SECURITY PROCESSES** All system hardware/software assets and their configuration deployed in the production system must be managed in a CMDB.

29.2 An onboarding and off-boarding process must exist to ensure only authorised users are provided with access to the system and the access is terminated when the user changes roles or leaves the company.

29.3 All changes/releases deployed into the pre-production/production environments must be controlled through a robust change management process.

29.4 A process should exist for controlling the regular deployment of patches into the productive environments in a timely manner.

29.5 All security incidents must be recorded, tracked through to closure and communicated to stakeholder following a security Incident Management Process.

29.6 The system must have a business continuity plan which is periodically tested to ensure the system can be recovered following a major incident.

29.7 The Supplier shall provide comprehensive security Testing to identify, assess, and mitigate security risks across the full lifecycle of the products, including infrastructure-as-code (IaC), container images, APIs, workloads, and runtime environments.

**30** **APPLICATION SECURITY INCIDENT MANAGEMENT** The Supplier will report, manage an actual or suspected breach of information security of the service in line with Home Office Digital policy.

**31** **SECURITY MONITORING** The Supplier will monitor the end-to-end security of the service and carry out monitoring on a regular basis as required to meet the required service levels.

31.2 This will include;

31.2.1 Contributing to identifying the systems, Configuration Items, or other service components that should be monitored and establishing the Security monitoring strategy.

31.2.2 Implementing and maintaining Security monitoring, using SIEM (Security Incident and Event Management) monitoring tools where relevant

31.2.3 Establishing and maintaining thresholds and other criteria for determining Security events, and choosing criteria to define each type of event (informational, warning, or exception)

31.2.4 Contributing to establishing and maintaining policies for how each type of detected event should be handled to ensure proper management. All high priority alerts must be raised in the mandated tools.

31.2.5 Implementing processes required to operationalise the defined thresholds, criteria, and policies.

31.2.6 Regular checks to ensure the Application has not breached or application not being attacked.

32 **SECURITY TOOLING** The Supplier will utilise security tooling as stated by the Buyer which includes, but not limited to;

32.2 [redacted]

32.3

32.4

32.5

33 **DESIGN SECURITY** The Supplier shall work collaboratively with the MBTP cyber security architects to ensure any design is secure and uses the Secure by Design Principles.

34 **ARCHITECTURE REQUIREMENTS** The Supplier must ensure that all systems are operated in such a manner that;

34.2 The CtB Products shall be able to monitor the operational health and usage of the applications and services used by the CtB Product Family.

34.3 The Supplier must comply with the Buyer's policies and the EU Directive on PNR Data and any applicable legislation.

34.4 The Supplier shall collaborate with the Buyer to establish cost monitoring processes and where appropriate cost controls for cloud capabilities within the product.

34.5 The Supplier will be required to follow and support the Buyer architectural and design governance practices.

34.6 The Supplier will be required to follow the Buyer's architectural and design standards.

34.7 The Supplier will be responsible for maintaining a technical debt register and review of the technical debt register with an appointed Buyer representative on a regular basis to report, manage and plan remediation of said technical debt. Current technical debt can be found at Annex 1

34.8 The Supplier is required to support and input to the architectural risk register which will be reviewed with an appointed Buyer representative monthly to report, manage and plan remediation of risk.

34.9 The Supplier will work with the Buyer in alignment with the HO Digital strategy (2030), roadmap, and priorities of the Crossing the Border product family.

34.10 The Supplier shall adhere to the overall architectural definition strategy led by Buyer-appointed forums such as the Technical Design Buyer (TDA) and its representatives.

34.11 The Supplier in collaboration with the Buyer shall assure all deliverables and products against the logical and physical architectures and environment designs are in accordance with the Buyer's Technical Design Buyer (TDA)

34.12 The Supplier will ensure that CtB products can be shut down and started independently of other Home Office products with zero data lost during controlled processes.

34.13 Unless deemed an emergency scenario the Supplier will be required to schedule any downtime for the CtB capability within agreed low traffic windows

35 **TESTING REQUIREMENTS** The Supplier shall ensure that all tests are included with the correlated code and configuration changes within the source and version control process.

35.2 The Supplier shall ensure that entire testing lifecycle is included within the automation pipeline with configuration criteria defining the scope and content of the test execution.

35.3 The Supplier shall ensure that as a minimum 80% of release regression packs are fully automated with the remainder being auto-assisted on manual intervention. Manual regression steps are to be agreed by exception.

35.4 The Supplier shall ensure that release performance tests are automated to verify that no unacceptable service degradations are released.

35.5 The Supplier shall adopt and subscribe to the Buyer's security testing processes and adopt a shift left approach in the delivery pipeline.

35.6 The Supplier shall ensure that code, test, and requirement coverage metrics are agreed and measured per component.

35.7 The Supplier shall ensure that no component is delivered that exceeds the agreed defect threshold and criteria for the related test phase.

35.8 The Supplier shall utilise the Buyer's defect classification model and record all related defect information within the Buyer's JIRA instance. Where the security classification of the defect prevents the utilisation of JIRA the Buyer will agree an alternate method with the Supplier.

35.9 The Supplier shall maintain and evidence test plans, execution results and completion reports for each iteration and at each tier of test. The format and content of said artifacts with be collaboratively agreed with the Buyer's Test Assurance Team.

35.10 The Supplier shall follow the Buyer's overarching test strategy and collaborate on any changes or enhancements required to support the product.

35.11 The Supplier shall adopt an ‘automation first’, ‘Shift Left’ test approach to support all Buyer products.

35.12 The Supplier shall conduct Soak Testing, ensuring the solution is capable of running for a sustained period without any issues so that the solution can maintain a level of performance and Availability over a sustained period.

35.13 The Supplier shall ensure their Testing services align with industry best practices

35.14 The Supplier shall collaborate with the Buyer to develop a test strategy and RACI for test stages (including support for Buyer test stages) as soon as practicable after the effective date but in any case, no later than 20 working days (or such other period as the parties may agree in writing) after the effective date and agree it with the Buyer.

35.15 The Supplier shall contribute to end-to-end Testing to include:

35.15.1 Providing test planning documentation (test cases, entry/exit criteria, dependencies)

35.15.2 Using the Buyer’s TDCS (test design and consultancy services) procedures, including Operational Acceptance Testing (OAT), Functional Acceptance Testing (FAT), User Acceptance Testing (UAT), Service Accreditation, Stress and Volumetric Testing and Service Readiness Testing (SRT).

35.15.3 Supporting the Buyer with end-to-end Testing to measure performance.

35.15.4 Supporting remediation of any identified issues identified during Testing

35.16 The Supplier shall provide comprehensive security Testing to identify, assess, and mitigate security risks across the full lifecycle of the products, including infrastructure-as-code (IaC), container images, APIs, workloads, and runtime environments.

**Non Functional testing**

36 The Supplier must implement performance and Load Testing of the Platform products, ensuring that the solution meets and all volumetric requirements.

36.1 The Buyer performance and Load Testing shall include normal, peak and stress loads to validate the volumetric requirements of the Platform products.

36.2 The Supplier shall support the Buyer in all planned assurance audit or witness Testing activities.

36.3 The Supplier shall support Buyer led, end to end, performance Testing by running a comprehensive performance test suite against the products

36.4 Where applicable, the Supplier must ensure that any Platform blocking bugs are Resolved in a timely manner agreed with the Buyer to run a comprehensive performance test suite against the Services before promotion to the live environment.

36.5 The Supplier shall measure latency, throughput, and resource utilisation across products.

36.6 The Supplier shall implement Observability measures and monitor to identify potential issues, trends or bottlenecks in compute, storage, and networking layers for all products.

## 37 PAYMENT AND INVOICING

37.1 Invoices for payment should be submitted monthly in arrears.

37.2 Invoices should only be raised for works delivered and approved by the Buyer as per the statement of work approval process.

37.3 Payment will only be processed on receipt of a valid invoice containing the relevant purchase orders details.

37.4 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

37.5 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

37.6 Invoices should be submitted to [redacted]

## 38 CONTRACT MANAGEMENT

38.1 The Supplier will be required to attend regular contract management meetings (monthly) where the following areas will be discussed;

38.2 Review and agreement of works to be completed (statement of works)

38.3 Supplier performance/KPI review

38.4 Review of delivery against key miles stones

38.5 Risk and issues

38.6 Please note this list is not exhaustive.

38.7 Attendance at Contract Review meetings shall be at the Supplier's own expense.

**39 LOCATION**

39.1 The Services will be carried out remotely with occasional travel required to Home Office locations within the UK. This includes, but is not limited to;

39.2 Face to face planning sessions

39.3 Buyer HO Digital events

39.4 Collaborative working sessions with Buyer HO Digital, incumbent supplier, suppliers within the CtB ecosystem, Buyer stakeholders and any other stakeholders as deemed appropriate by the Buyer.

39.5 The Supplier will be responsible for all costs for travel which is required to enable the successful delivery of the Services, including out of hours requests.

Crown Commercial Service

## Attachment 2 – Charges and Invoicing

Charges are based on the information and assumptions contained in the Supplier's Response and any changes agreed during the contract engrossment period with the Buyer.

[redacted]

Crown Commercial Service

## Part A – Milestone Payments and Delay Payments

| # | Milestone Description | Milestone Payment amount (£GBP) plus VAT | Milestone Date and billing frequency | Delay Payments (where Milestone) (£GBP per day) |
|---|---|---|---|---|
| M1 | Discovery and Mobilisation<br>08/12/2025 – 30/06/2026 | [redacted] | | |
| M2 | Implementation Period (estimated to be 01/07/2026 – 07/12/2026) | | | |
| M3 | Year 2 BAU Service Delivery (08/12/2026 – 30/06/2027). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of Year 1. | | | |
| M4 | Year 2 BAU Service Delivery (01/07/2027 – 31/12/2027). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M3. | | | |
| M5 | Year 3 BAU Service Delivery (01/01/2028 – 30/06/2028). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M4. | | | |
| M6 | Year 3 BAU Service Delivery (01/07/2028 – 31/12/2028). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M5. | | | |
| M7 | Year 4 BAU Service Delivery (01/01/2028 – 30/06/2029). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M6. | | | |
| M8 | Year 4 BAU Service Delivery (01/07/2029 – 31/12/2029). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M7. | | | |
| M9 | Year 5 BAU Service Delivery (01/01/2030 – 30/06/2030). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M8. | | | |

Crown Commercial Service

| | |
|---|---|
| M10 | Year 5 BAU Service Delivery (01/07/2030 – 08/12/2030). Milestones to be agreed in line with PI planning and Payment in line with contract value will be agreed by the end of milestone M9. |

[redacted]

**Part B – Service Charges**

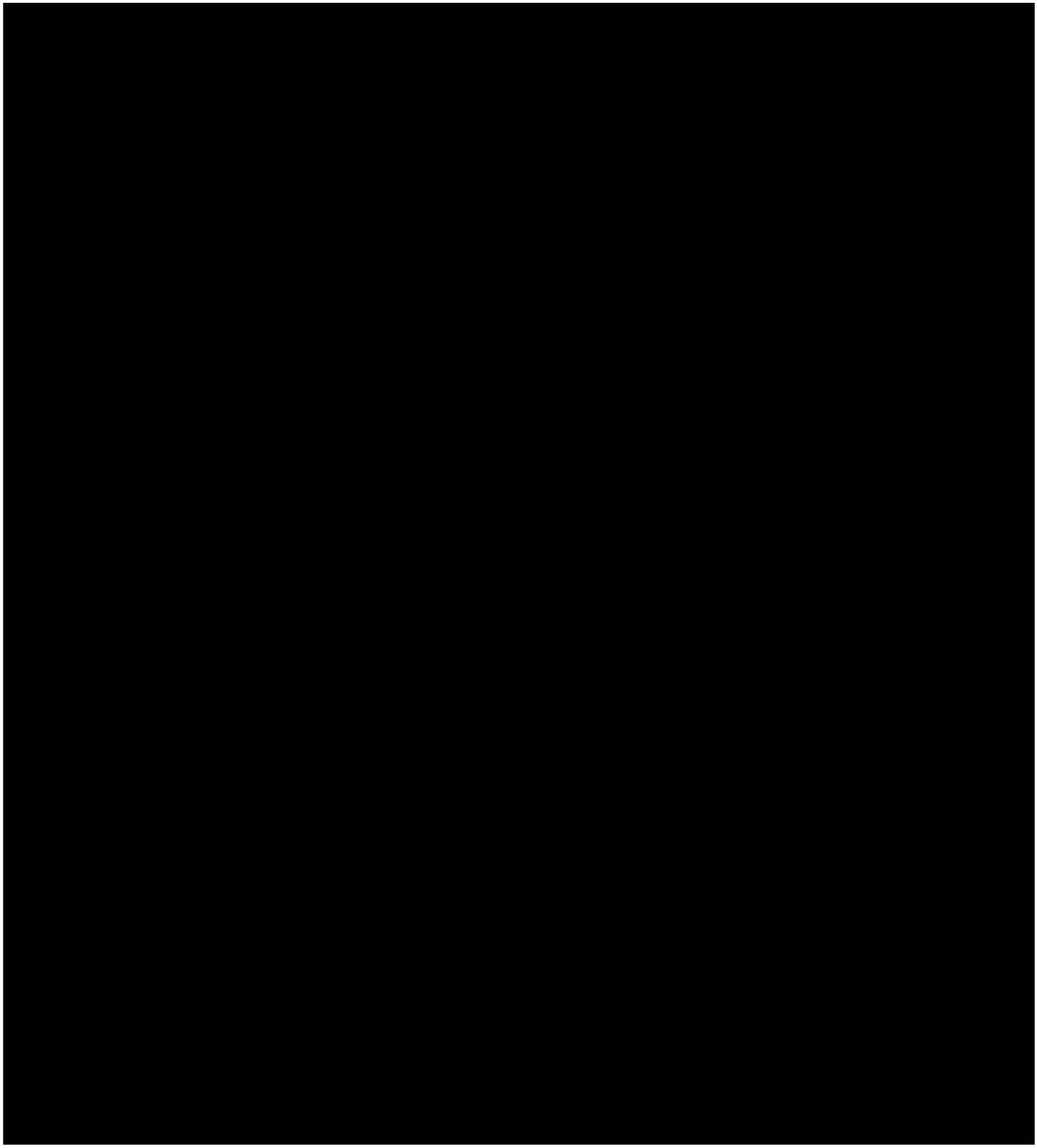
[redacted]

Crown Commercial Service

| | |
|---|---|
| **BAU Service Delivery**<br>Estimated Start: 08/12/2026 | [redacted] |

[redacted]

Crown
Commercial
Service



Crown Commercial Service

[redacted]

## Part E – Early Termination Fee(s)

Early termination fees will be calculated as 6 x the Supplier's agreed monthly run rate. The Supplier's monthly run rate will be agreed ahead of each Contract Year.

Crown Commercial Service

## Attachment 3 – Outline Implementation Plan

Crown Commercial Service

## Attachment 4 – Service Levels and Service Credits

**Service levels and service credits will be agreed during the Discovery and Mobilisation Period.**

### SERVICE LEVELS AND PERFORMANCE

Service levels and service credits will be agreed once the transition period has concluded. Annual check points will be undertaken throughout the contract lifecycle where the service levels and service credits of the following year will be agreed.

### Service Levels and Service Credits

| Service Levels | | | | Service Credit for each Service Period |
|---|---|---|---|---|
| **Service Level Performance Criterion** | **Key Indicator** | **Service Level Performance Measure** | **Service Level Threshold** | |
| Relief given through Discovery and Mobilisation | Relief given through Discovery and Mobilisation | Relief given through Discovery and Mobilisation | Relief given through Discovery and Mobilisation | Relief given through Discovery and Mobilisation |

The method for Service Credits shall be agreed by the end of the Discovery and Mobilisation period.

### Service Credit Cap

The Service Credit Cap shall be agreed by the end of the Discovery and Mobilisation period.

### Critical Service Level Failure

Critical metrics will be agreed by the end of the Discovery and Mobilisation Period.

Crown Commercial Service

## 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

[redacted]

### Part B – Key Sub-Contractors

| Key Sub-contractor name and address (if not the same as the registered office) | Registered office and company number | Related product/Service description | Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period | Key role in delivery of the Services |
|---|---|---|---|---|
| AppVia Limited | [redacted] | | | |

Crown Commercial Service

## Attachment 6 – Software – Not Applicable

## Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

**PART A – CREDIT RATING THRESHOLD**

| **Entity** | **Credit Rating (long term)**<br>*(insert credit rating issued for the entity at the Commencement Date)* | **Credit Rating Threshold**<br>*(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3)* |
|---|---|---|
| **Kainos Software Limited** | [redacted] | |
| **AppVia Ltd** | | |

**PART B – RATING AGENCIES**

- Dun and Bradstreet
  - 100-86 Minimal Risk
  - 85-51 Lower than average risk
  - 50-11 Greater than average risk
  - 10-0 High Risk
- Company Watch
  - 100-36 Low risk
  - 35-26 Greater than average risk
  - 25-0 High risk

- Attachment 8 – Governance

**PART A – SHORT FORM GOVERNANCE – Not Used**

**PART B – LONG FORM GOVERNANCE**

Long form governance will be agreed once the Discovery and Mobilisation Period has concluded. Annual check points will be undertaken throughout the contract lifecycle where the long form governance for the following year will be agreed. During the course of Discovery and Mobilisation the Parties will operate at a minimum of two governance boards:

1 Weekly delivery working group – to be run by the Supplier to provide the Buyer with delivery progress reports and to discuss and agree mitigations to any risks and issues.

2 Monthly supplier performance review – to be run by the Supplier Engagement Lead and to include an overview of the Supplier's delivery and progress against the payment Milestones.

## 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] Officer, [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 Buyer is Controller and the Supplier is Processor**<br><br>The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:<br><br>• The Supplier will not have access to any personal data during the course of the services other than contact details required to communicate with the Buyers staff. |
| Duration of the processing | For the full duration of the contract, 48 month plus the 12 month extension period, if invoked. |
| Nature and purposes of the processing | Not applicable as the Supplier is not accessing any personal information. |
| Type of Personal Data | Not applicable as the Supplier is not accessing any personal information. |
| Categories of Data Subject | Not applicable as the Supplier is not accessing any personal information. |
| 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 | Not applicable as the Supplier is not accessing any personal information. |

## Attachment 10 – Transparency Reports

During the Discovery and Mobilisation period a weekly status report will be delivered in PowerPoint format to an agreed list of Buyer stakeholders. Transparency Reports for the Implementation Period will be agreed once the Discovery and Mobilisation period has concluded.

# ANNEXES

## Annex 1- Tech Debt

CtB Tech Debt and Future Reqs v1.0 (1).d

## Annex 2 – Governance and Forums

CtB Governance and Operational Forums v

CtB Products, Services and Support

CtB Processes

## Annex 3 - Suppliers Response

Qualification Envelope.pdf

Lot 2 Technical Questions T1 MISSIO

Lot 2 Technical Questions - T2 SUPP

Lot 2 Technical Questions - T3 TECH

Lot 2 Technical Questions - T4 TEST

Lot 2 Technical Questions - T5 APPR

Lot 2 Technical Questions - T6 MONI

Lot 2 Technical Questions - T7 FREQL

Lot 2 Technical Questions - T8 SOCIA

Generic Technical Questions - T1 SUPPL

Generic Technical Questions - T2 DELIVE

Generic Technical Questions - T3 DELIVE

Generic Technical Questions - T4 DELIVE

Generic Technical Question T5 STANDA

Generic Technical Questions - T6 GOVEF

Generic Technical Questions T7 SOCIAL

CtB Products and Services Price Schedu

Assumptions.pdf

## Annex 4– Call Off Terms and Additional/Alternative Schedules and Clauses

RM6100-Lots-2-3-and-5-Call-Off-Terms- 2

RM6100-Lots-2-3-and-5-Additional-and-A

## Annex 5 – Product list

Border Platforms - Product Transition Lis