Crown Commercial Service

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

Home Office
Crossing the Border Products and Services
Level 2 Support contract with IBM Contract
Reference: C9667-B

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated [2nd February 2026] between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website RM6100 Technology Services 3. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

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

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

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;

Crown Commercial Service

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. RM6100 Order Form – Lots 2, 3 and 5
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.
13. Annex 2 – Call Off Special Terms
14. Annex 3 – Security Aspects Letter

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

.1.1 the Framework, except Framework Schedule 18 (Tender);

.1.2 the Order Form;

.1.3 the Call Off Terms; and

.1.4 Framework Schedule 18 (Tender).

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
BAU	means business as usual
Border Force	means the Buyer directorate responsible for control of the UK border
BPSS	means the government Baseline Personnel Security Standard as detailed at National security vetting: clearance levels - GOV.UK (www.gov.uk)
BX	means the Border Crossing (BX)product which is made of several parts - Primary 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.
Buyer	means Secretary of State for the Home Department, acting on behalf of the Home Office

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	date set out at Section A of this Order Form
Conformance Point	means a defined time in the Mobilisation / Transition Period process, where compliance with a defined specification or requirement is measured or enforced For clarity, the Conformance Point dates are as follows: Initial review: 31st July 2026 End of Year 1: 31st December 2026 End of Year 2: 31st December 2027 End of Year 3: 31st December 2028 End of Year 4: 31st December 2029 End of Year 5: 31st December 2030
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 Term	means the term of the contract awarded as a result of this procurement, in this instance 3 years and 11 Months plus an optional 1 year extension
CSV	means comma separated values
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 accessed 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

Data Operations	means the Buyer Data Operations Team
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
EBSA	means the Authorities Environment Build Support Administration platform
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
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	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)
HO Digital	Referred to as HOD, means the Home Office Digital Directorate which provides the Buyer's internal and external facing IT and digital services
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.

Crown Commercial Service

Implementation Period	means the timeframe during the first contract year following the Mobilisation / Transition period to the end of the first contract Year where all agreed-upon actions, deliverables, and milestones are carried out according to the established schedule. 1st May 2026 to 1st January 2027

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 have been unable to resolve. Level 2 support involves indepth 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 which deliver a digital and technology services for the protection of the UK border
Mobilisation/Transition Period	means the period following contract award where the Supplier will onboard and establish the detail required for transition and implementation of Services and develop the final service delivery plan and is a distinct phase prior to implementation of the services into BAU
Negative Immigration	means an Immigration watchlist, one of the watchlists within Helios
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)
NPPV3	means Non Police Personnel Vetting level 3. It permits access to Secret level material. As detailed: About the Police National Vetting Service | Warwickshire Police

O Side	means the cloud-based platform used to hold data marked as Official
Parties	means the Buyer and the Supplier
PKI Certificates	means Public Key Infrastructure (PKI) certificates. These 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
Potential Provider	means a company or other entity that submits a Tender in response to the Further Competition Invitation
Preferred Provider	means the Potential Provider with the highest total average score after evaluation of Potential Provider technical and price bids;
Problem Management	means the process of identifying, managing and finding solutions for the root cause of incidents on an IT service.
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
Product Manager	means the person(s) responsible for the strategic direction of products and services for the Buyer;
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
Root Cause Analysis	means the process of identifying and solving problems/issues after occurrence.
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 Management	means the management and delivery of Crossing The Border services that meet the Buyer's business needs as defined in the Buyer's requirements, focusing on incident/problem/change/service request management and continual improvement.
Service Integrator	means the Supplier acting on behalf of the Buyer to coordinate multiple IT suppliers and internal teams to deliver seamless, cohesive crossing the border services, ensuring different systems and suppliers within the CTB ecosystem work together efficiently under a central management framework to improve value and service delivery.
Service Go Live Date	1st May 2026
Service Transition	means Service transition lifecycle stage makes sure that changes to services and service management processes are carried out in a coordinated way. The Buyer team is responsible for working with delivery teams on transitioning releases into live support
SFTS	means securities financing transactions
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
SWG	means security working group
SyOps	means systems operation and IT operations management
Services	means the services outlined in this Attachment 1 Service Requirements document
Transition Premises	means the location for carrying out transition activities during the Mobilisation/Transition period

UI	means user interface
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 Monday to Friday 08:00 to 17:00 excluding public holidays

Section A General information

Contract Details	
Contract Reference:	Itt_77424
Contract Title:	Crossing the Borders Lot 3b – Level 2 Support
Contract Description:	Provision of Level 2 Support, Management and maintenance for Crossing the Border Ecosystem
Contract Anticipated Potential Value this should set out the total potential value of the Contract	£8,721,260.14

Crown Commercial Service

Estimated Year 1 Charges:	[redacted]

Commencement Date: 02 February 2026

Buyer details

Buyer organisation name
Secretary of State for the Home Department, acting on behalf of the Home Office (referred to as "Buyer")

Billing address

2 Marsham Street,
London,
SW1P 4DF

Buyer representative name

[redacted]

Buyer representative contact details

[redacted]

Buyer Project Reference
Project -75566

Crown Commercial Service

Supplier details
Supplier name IBM United Kingdom Limited , Company Registration number 00741598 (referred to as the “Supplier”)
Supplier address [redacted]
Supplier representative name [redacted]
Supplier representative contact details [redacted]
Order reference number or the Supplier’s Catalogue Service Offer Reference Number Not Applicable

Guarantor details
Guarantor Company Name Not Applicable
Guarantor Company Number Not Applicable
Guarantor Registered Address Not Applicable

Crown Commercial Service

Section B Part A – Framework Lot

Framework Lot under which this Order is being placed

1.	TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2.	TRANSITION & TRANSFORMATION	☐
3.	OPERATIONAL SERVICES	
	a: End User Services	☐
	b: Operational Management	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

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	Not Applicable
3	59 (4 years and 11 months)
5	Not Applicable

Initial Term Months 47 months

Extension Period (Optional) Months 12 months

Crown Commercial Service

Minimum Notice Period for exercise of Termination Without Cause 6 months (183 calendar days)

Sites for the provision of the Services

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

2 Ruskin Square,
Dingwall Road,
Croydon,
CR0 2WF

Supplier Premises:

[redacted]

[redacted]

Third Party Premises:
Not Applicable

Crown Commercial Service

Buyer Assets

Details of Buyer Assets have been derived from **Attachment 1 – Services Specification.**

These include:

1. [redacted]
2. Provision of access to Buyer-owned software and tooling, including but not limited to:
   - ServiceNow
   - Sharepoint
   - Confluence
   - Atlassian suite (Jira)
   - Connectivity software to Home Office CtB environments (e.g. VPN)
   - Dynatrace, Prometheus, Grafana, CloudWatch for AWS, ELK
   - Slack
3. Provision of Buyer-supplied laptops.
   - POISE
4. Provision of Buyer-owned onboarding mandatory training materials.

Additional Standards

Additional standards may be agreed by the Parties, acting reasonably, prior to the start of the Year 1 Implementation Period.

Buyer Security Policy

The Supplier will adhere to the following Government and Departmental Processes, Policies and Standards:

- Secure By Design - Secure by Design - UK Government Security
- UK Government Security and Cyber policies

The Supplier is required to comply with all Buyer Security & Cyber Policies shared with the Supplier at ITT phase and during engrossment.

The parties agree that the Buyer security and cyber policies provided to the Supplier at these stages may be subject to change throughout the life of the contract as processes develop. The Supplier will comply with any relevant updated security and cyber policies as updated.
The Supplier is also required to comply with the Security Aspects Letter in Annex 13 of this Order Form.

Crown Commercial Service

Buyer ICT Policy

- Home Office Digital Strategy: https://www.gov.uk/government/publications/home-office-digital-strategy/home-officedigital-strategy Home Office Technology Strategy: https://www.gov.uk/government/publications/home-office-technology-strategy/homeoffice-technology-strategy

Government Service Design Manual: https://www.gov.uk/service-manual

Insurance

Third Party Public Liability Insurance (£) 5,000,000 in respect of any one claim and in the aggregate per annum.
Professional Indemnity Insurance (£) 1,000,000 in respect of any one claim and in the aggregate per annum.

Buyer Responsibilities

Listed below are the dependencies on the Buyer for the Level 2 Support Mobilisation/Transition Period.

A full list of dependencies for Implementation will be agreed by the Parties, acting reasonably, prior to the start of the Year 1 Implementation Period.

Annual check points will be undertaken throughout the contract lifecycle where the required outcomes for the following year will be agreed. These are referred to in this Order Form as conformance points; the initial Conformance Point following the end of the Mobilisation / Transition Period will be by 31st July 2026. The first yearly Conformance Point will be at the end of the Implementation Period and then annually thereafter.

In addition to annual Conformance Points 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 changes to the scope of Services is required. Any Changes to the scope of Services will be subject to the Change Control process pursuant to Schedule 5 (Change Control Procedure). If the ticket volumes are exceeded in any month, Service Credits will not be applied to those tickets within the month exceeding the volume specified. Irrespective of this, the Supplier shall continue to operate within the proposed Service Levels.

Crown Commercial Service

The Buyer will meet the following responsibilities during the Mobilisation / Transition Period. In the event that any of these Buyer Responsibilities are not met then the Supplier is relieved from liability for achieving the affected Deliverables in table 5 - the Supplier Deliverables Required for Transition in Attachment 3. The Parties shall, acting reasonably, agree on adjustment to dates, deliverables or reprofiling of the agreed payment schedule as applicable.

In addition to these Buyer Responsibilities, core assumptions are documented in Attachment 1 Scope of Services and Services Description.

Table 1: Buyer Responsibilities

BR1	Overall management and responsibility for all third-party suppliers that are involved in the CtB Level 2 transition. The Buyer may delegate the responsibility to the Service Integrator.
BR2	The Buyer to ensure the incumbent supplier provides all baselined existing CtB support documentation prior to transition commencement, this refers to existing artefacts maintained by the Buyer's incumbent supplier including but not limited to support processes and procedures, runbooks, automated fixes, historical incidents with remediation information, SOC operating procedures, Governance. The parties accept that additional documentation may be produced and shared with the supplier during the Mobilisation / Transition Period.
BR3	Ensure that all support teams (including but not limited to Level 3) are using the same ITSM tooling (Service Now) during Mobilisation / transition period.
BR4	[redacted]
BR5	Provide the Roles and Responsibilities of the System Integrator in relation to all aspects of the CtB Level 2 Service during Mobilisation/Transition Period.
BR6	Support the timely sponsorship of all security clearances as required.
BR7	Provide Onboarding Support including but not limited to the provision of support IDs, S* IDs, email, and are aligned to the agreed CtB Level 2 transition schedule.
BR8	Provide a Single Point of Contact throughout the transition period.
BR9	Provide access to all environments to deliver the CtB Level 2 Service, including but not limited to the Test, Training and Production environments.
BR10	Provide access and training for all systems and tooling to deliver the CtB Level 2 Service, including but not limited to, monitoring, reporting, ITSM, deployment and automations.

BR11	Provide contact details for all teams and individuals required to provide CtB Level 2 Support. This includes but is not limited to support queue details, hours of service and OOH cover, before Service Go Live Date.
BR12	Provide a copy of the Buyer's ITSM plan which includes the BCDR aspects (relates to requirement 24.1 as defined in Attachment 1) during transition so that the Supplier's business continuity plan can be agreed during transition.
BR13	Ensure provision of all existing alert documentation with resolution scripts (relates to requirement 22.2 as defined in Attachment 1), before Service Go Live Date.
BR14	Provide a change management function for the CtB Service (including but not limited to, the provision of the forward schedule of change, Change Approval Board, etc) from Service Go Live date.
BR15	Provide the Buyer Test Strategy to the Supplier (relates to requirement 55.1 as defined in Attachment 1)
BR16	Provide details of the MBTP End User Device Agreement. (relates to requirement 59.1 as defined in Attachment 1)
BR17	Provide information on CtB Level 2 relevant change activities / roadmap planned during transition (e.g. change freezes)
BR18	Ensure Buyer and Buyer's incumbent supplier staff, tools and infrastructure are available when needed for the planning and mobilisation phases.
BR19	Provide POISE laptops and access, to permit the Supplier to carry out the CtB Level 2 Transition and service.
BR20	Manage and ensure delivery from other suppliers of all design and code changes driven from an incident. (relates to requirements 10.5 and 10.6 as defined in Attachment 1) from Service Go Live Date.

Crown Commercial Service

Supplier Responsibilities

Table 2: Supplier Responsibilities

SR1 Communication and Collaboration	Work closely with the incumbent supplier and participate fully in transition planning and provide status updates to the Buyer.
SR2 Risk Management	Identify potential risks in the transition process, propose mitigation strategies and monitor risk throughout the transition.
SR3	Develop a detailed transition plan aligned with Buyer's objectives and timelines.
SR4 Knowledge Transfer	Participate in knowledge transfer sessions with the incumbent supplier, review and validate documentation, processes and system details and identify gaps and request clarifications promptly.
SR5 Resource mobilisation	Deploy skilled personnel for transition activities and ensure their staff are trained and ready for operational handover.
SR6 Service Readiness	Ensure compliance with contractual and security requirements are met, complete all knowledge transfers required and establish monitoring and reporting mechanisms and perform testing of readiness prior to Service Go Live Date.

Goods

Not Applicable

Governance – Option Part A or Part B

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

The Part selected above shall apply this Contract.

Crown Commercial Service

Change Control Procedure – Option Part A or Part B

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	☐
Part B – Long Form Change Control Schedule	**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):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £1500; and
- for the purpose of Paragraph 8.2.2, the figure shall be £100,000
- Any changes above the stated values above will be agreed with the Buyer and approved through the change control process.

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*

Part A – Additional Schedules

Additional Schedules	Tick as applicable
S1: Implementation Plan	**X**

Crown Commercial Service

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

Additional Clauses	Tick as applicable
C1: Relevant Convictions	x
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

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

Crown Commercial Service

Additional Schedule S3 (Security Requirements)

Crossing the Border L2 Support - Security

The Supplier draft Security Management Plan is inserted here a final Security Management plan will be agreed during Mobilisation / Transition Period to ensure compliance with Buyer Security requirements,

Security Aspects Letter and security policies would be reviewed as necessary throughout the Contract term.

Additional Schedule S4 (Staff Transfer)

CtB%20contract%20-%20Staff%20Transfer

Crown Commercial Service

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;

❖ 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:

- HMRC successfully challenging the Potential Provider under the General Anti – Abuse Rule (GAAR) or the "Halifax" abuse principle; or
- a tax authority in a jurisdiction in which the Potential Provider 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;
- a failure to notify, or failure of an avoidance scheme which the Potential Provider 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 Potential Provider is established.

Other offences

❖ Any other offence within the meaning of Article 57(1) of the 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 Directive created after 26th February 2015 in England, Wales or Northern Ireland.

Crown Commercial Service

Additional Clause C3 (Collaboration Agreement)

[redacted]ence
[redacted]ence

A Collaboration Agreement from the Buyer has been provided to the Supplier. Collaboration Agreement will be agreed within the first 30 days following the final contract commencement of the CtB Lot Providers (BAE, IBM, Kainos). The Buyer will notify all dependent contracts of commencement date of the Collaboration Agreement.

Crown Commercial Service

Section D Supplier Response

Lot 3 T1.docx Lot 3 T2.docx Lot 3 T4.docx Lot 3 T3.docx

Commercially Sensitive information

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 methodologies and approaches.

Charging and Invoicing (Attachment 2)- Prices and charges contained in the tender and contract are commercially sensitive.

IBM Bid Submission (Attachment 1):

- Supplier Reference projects and clients described in all responses.

Where disclosure is deemed necessary to comply with the terms of the Act, the Supplier requests that at least fourteen (14) days prior notification be provided to the Contractor with details of the requesting party.

Section E Contract Award

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

SIGNATURES

Crown Commercial Service

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		

Attachment 1 – Services Specification

5. SERVICE LEVELS AND PERFORMANCE

The Supplier will work to resolve Incidents within the targets detailed below.

The Parties have agreed the Service Levels below which will apply from the Service Go Live Date and throughout the Implementation Periods.

5.1 The Service Levels tables below are for Production/ESIT environments:

The Supplier will provide support in the hours detailed below:	
Service Hours - ESIT/ Production Environment	24 /7
Security Incident	24/7
Training Environment	Mon-Sun 08:00 – 20:00, including UK public holidays

The Supplier will work to resolve Incidents within the targets detailed below:

Priority	Description	Response Target	Resolution Target

P1	P1 means an Incident: a) that results in a complete or substantial loss of the Service; or (b) that results in an essential part of the Service being unusable for all End Users; or (c) that results in all End Users being unable to access the Service.	100% <= 15 mins	100% <= 4 hours
P2	P2 means an Incident: (a) where the Service is materially adversely affected, but can be circumvented; or (b) where the Service remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of End Users is unable to access the Service; or certain material aspects of the Service.	100% <= 30 mins	100% <= 8 hours
P3	P3 means an Incident: (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 (b) affecting a single or small group of End Users.	100% <= 24 hours	95% <= 2 Working Days 100% <= 5 Working Days
Priority	Description	Response Target	Resolution Target
P4	P4 means an Incident: (a) that results in little or no material impact on the Service or the Customer's business; or (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.	100% <= 48 hours	95% <= 3 working days 100% < 5 working days

5.2 The following table is for non-production environments which include Training Environment

Priority	Description	Resolution Target
P1	N/A	N/A

P2	P2 means an Incident: (a) that results in a complete or substantial loss of the Environment; or (b) that results in an essential part of the Environment being unusable for all Users; or (c) that results in all Users being unable to access the Environment (d) impacts the ability to deploy releases or fixes into Production (e) impacts the velocity of the delivery teams	100% 8 hours (within Operating Hours)
P3	P3 means an Incident: (a) where the Environment is materially adversely affected, but can be circumvented; or (b) where the Environment remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of Users are unable to access the Environment; or certain material aspects of the Service	100% within 3 working days
P4	P4 means an Incident: (a) that results in a minimal impact for the Service where non-critical functions or procedures are down, unusable, or difficult to use; or (b) affecting a single or small group of End Users.	100% within 5 working days

5.3 The following Service Levels are for Security incident management:

Priority	Description	Response Target	Resolve Target
P1	P1 means an Incident: Any Incident which may cause the degradation of vital service for a large number of users, involve a serious breach of network security, affect mission critical equipment or services or damage public confidence in the Government.	15 minutes	100% <= 4 hours
P2	P2 means an Incident: Incidents which are not Critical, and which may impact a smaller group of Users, disrupt nonessential services, breach network security policy or affect the reputation of Government bodies and services.	30 minutes	100% <= 8 hours

P3	P3 means an Incident: Incidents which are neither Critical, nor High and which can be handled by local IT and security offices. These Incidents do not typically impact IT services and include examples such as unsuccessful denial-of service attacks or the majority of network monitoring alerts.	24 hours	95% <= 2 Working Days 100% <= 5 Working Days
P4	P4 means an Incident: Incidents, which are not Critical, High nor Medium and are in general considered to be part of normal IT support operations. These incidents would include receipt of an isolated SPAM or anti-virus alert, minor computer hardware failure, loss of network connectivity to a peripheral device or loss of access to an external, non-essential service.	48 hours	95% <= 3 working days 100% < 5 working days

5.4 The following Service Levels apply for CTB Service request/account management:

Request Type	Support Hours	SLA
Account Creation	09:00-17:00, Monday to Friday excl. PH's	5 working days
Amend (role change)	09:00-17:00, Monday to Friday excl. PH's	5 working days
Disable/Re-enable (role change, name change, update SC expiry date)	09:00-17:00, Monday to Friday excl. PH's	5 working days
Account Unlock	24/7	4 hours

Buyers's Requirement issued at ITT

Lot 3 Technical Questions

Crown Commercial Service

How%20to%20Bid%20BX%20Helios%20B

SCOPE OF SERVICES AND SERVICES DESCRIPTION

The Supplier and Buyer ran an engrossment period during which both Parties further defined and agreed a set of initial scope for the Supplier which is laid out in section 2 of this Attachment 1. These defined requirements scope in attachment 1 supersedes the scope of requirements issued in ITT number 77424, Crossing the Borders (hereafter referred to as CtB) Lot 3 for the Mobilisation / Transition Period. All other information published in the ITT remains applicable and in scope.

Engrossment also established the need for a 12-week Mobilisation / Transition Period to clarify the ongoing level 2 support service that the Supplier will provide to the Buyer during the Implementation Period. A review will be carried out at the end of the Mobilisation / Transition Period to agree a final scope including volumetrics.

Attachment 1 sets out a detailed scope of services for the Mobilisation / Transition Period. The output of this transition period and the discovery period for the other contracts within the ecosystem will inform a Conformance Period which will run and will conclude with a check-point during which any change of scope of services and committed deliverables of the Supplier will be jointly considered and agreed for the remainder of Year 1 during the Implementation Period and where applicable the contract period.

During the Mobilisation/ Transition Period the Buyer and Supplier, working with the Service Integrator will agree on Key Performance (KPI) metrics and Service Levels including Service Credits and the 1% behaviour incentive scheme.

Where joint agreement cannot be reached on the final scope of Services and committed Deliverables on completion of the transition and discovery periods, both Parties agree that the matter will be resolved using the Dispute Resolution Procedure, if appropriate, or by other means to reach agreement, for example through escalation within each organisation. The Service will continue as agreed under the existing Order Form until joint agreement is reached.

The Supplier will provide a consistent and frequent Service Management presence on site and other Supplier team members will be required to attend Buyer locations as jointly deemed necessary by the Buyer and Supplier, for example, when planned meetings require face to face attendance, face to face planning sessions, Buyer HO Digital events, collaborative working sessions with Buyer HO Digital suppliers within the ecosystem, incumbent supplier, Buyer stakeholders and any other stakeholders as deemed appropriate by the Buyer . Please note that this list is not exhaustive.

The Buyer will inform the Supplier when additional site attendance is required beyond the regular attendance at Buyer's locations for the purposes of delivering the Service during the term of this Contract.

Crown Commercial Service

[redacted]

Scope : Requirement Solution Alignment

The Requirement ID in the below relates to the numbering within the requirements document issued at ITT.

Table 3 – In Scope Requirements of the CTB Level 2 Service

Req ID	Requirement	Jointly agreed requirement scope
6.1.1	Support code deployments into Integration test and Production environments via the Buyer's change and release process.	[redacted]
6.1.2	Support the Buyer live service, including timely and effective remediation for incidents and problems to meet service level agreements.	[redacted]

		[redacted]
6.1.3	Ensure a dedicated team is responsible for providing support to the Product Family.	CtB Level 2 Services will be delivered using a Shared Services Team delivering similar services for multiple secure projects and services of the Buyer.
6.1.4	Work with delivery teams, support teams, and Buyer BAU Live Services Operational Teams collaboratively and co-operatively.	Accepted.
6.1.5	Support and conform to the Buyer's governance processes.	Accepted.
6.1.6	Participate in flexible working practices.	Accepted.
6.1.7	Provide progress and performance information and service reports as required.	In accordance with those performance reports listed in the Order Form and/or as subsequently and jointly agreed by both parties.
6.1.8	Work with the Buyer at appropriate stages of delivery from pre-discovery investigation, through discovery, impact assessment, delivery, integrated testing, service transition into live service operations, deployment into production and early life support.	Accepted.
6.1.9	Impact assess requirements as per the new demand process.	Accepted.
6.1.10	Deliver a flexible, responsive service provision, supporting the delivery of the objectives and priorities set out above via the product family.	Accepted.

6.1.11	Work in partnership with all stakeholders in HOD and its partners in an atmosphere of openness and transparency.	Accepted.

7.1	The application will be handed over to The Supplier in an iterative manner. Potential Provider will provide ongoing support for the CtB Product Family.	Accepted.
7.2	The Supplier shall work collaboratively with multiple Suppliers and act as the conduit for all BX S* incidents for the end-to-end service. The Supplier's role shall be pivotal in performing the initial triage and determining the areas or parties involved. The Supplier needs to understand the end-to-end service i.e. from the Ports, through Networks, platforms, application and data layers and external interfaces and data sources with external agencies. This will include:	Accepted.
7.2.1	Co-design of service management processes	Supplier is not responsible for co-design but will input as part of continuous improvement.
7.2.2	Participation in a fully Integrated ITIL 3/4/Product Centric based Service Delivery	Accepted.
7.2.3	Collaborative working with the Buyer and other Suppliers (first line support, Official side support, DevOps etc) to attain the end-to-end SLAs for the applications	Accepted.
7.2.4	Agreement of hand-offs across Supplier boundaries	Accepted.

7.2.5	Joint analysis and resolution of problems and suggestion of improvements	Accepted.
7.2.6	Collaborative participation in multi-supplier change boards.	Accepted.
7.3	The Supplier shall:	Accepted.
7.3.1	Align to ITIL methodology and integrate with HO ways of working.	Accepted.
7.3.2	Support the service management functions to meet perfor-	Accepted.

	mance, cost and functional service obligations delivered by the CtB Product Family.	
7.3.3	Ensure that service support processes include integration with the Buyer service support processes, including service desk; incident management; problem management; change management; release and deployment management; event management; major incident management; knowledge management; access management; service request management, configuration management (at a later date) and security incident management.	Accepted.
7.3.4	Include the following service delivery processes in their support: service level management; availability and performance reporting; IT service continuity management; security management; continuous service improvement; service reporting; service transition.	Accepted.

7.3.5	Collaborate with the Buyer Service Design/Transition team, development and test teams to complete impact assessment and early analysis of new features, enhancements as per CtB products roadmaps. This may include proposed improvements to develop the initial business requirements.	The Supplier will collaborate where applicable to deliver associated Level 2 Services.
7.3.6	Support the challenges of systems, data, and transitional architecture in a cross-cutting multi supplier environment.	Accepted.
7.3.7	Align to the Buyer product lifecycle methodology and toolsets as appropriate.	Accepted.

7.3.8	Monitor and develop metrics to demonstrate progress/ performance of the CtB Product Family services.	Accepted. For clarity this relates to the reporting of service trends and performance.
7.3.9	Work with the Buyer's service transition team to transition new demand and features into live services teams.	Accepted.
7.3.10	Be required to provide a copy of acceptance into service checklist for new Services as per demand pipeline, to show Potential Provider readiness.	Accepted.
7.3.11	Drive continuous improvement for the CtB Product Family.	Accepted.
7.3.12	Identify and support the Buyer to address resilience concerns.	Accepted.
7.3.13	Review CtB products' monitoring and reporting capability which will include improvements in monitoring to reduce time for support team to complete investigation.	Accepted.

7.3.14	Support initiatives to reduce deployment downtime.	Accepted.
7.3.15	Support the Buyer test approach/ strategy and provide resources as appropriate for the testing of all deliverables before release to production through change control.	The Supplier will support the Buyer test approach and strategy where appropriate to deliver the associated Level 2 Services.
7.3.16	May be required to engage and support external partners.	Accepted.
7.3.17	Support updates, patches, and security vulnerability fixes via the Buyer's change and release processes.	Accepted. The Supplier will be responsible for deployment of security patches and vulnerability fixes. These will be packaged into releases and tested by the Level 3 Support / Development Team / Platform team/QAT teams as appropriate.
7.3.18	Support integrated testing with interfacing products and services.	The Supplier will support testing where appropriate to deliver the associated Level 2 Services.
7.3.19	Use Dynatrace, Prometheus, Grafana for monitoring and alerting to Slack, with Cloud-Watch for AWS native resources. ELK is used for log aggregation and alerting of business events	Accepted.
10.1	The Supplier will provide Level 2 support capability in accordance with the Buyer ways of working.	Accepted.
10.2	These issues will be triaged and resolved by Level 2 and the Buyer's Level 3 support teams, utilising service knowledge and Instructions for known errors.	Accepted.

10.3	If The Supplier is unable to resolve an incident at Level 2 because it would require a change in the source code or a change in the way the product functions, data errors, or is overall too technically complex; the incident will be raised via the Buyer's delivery toolset for investigation and resolution by Level 3.	Accepted.
10.4	Root Cause Analysis – Assist the Buyer Incident Management Team in providing an impact assessment on the cause of the issue, the impact to end users and support in resolving the issue.	Accepted.
10.5	Code Change – During an incident if identified by the Supplier, or product team a code change is required, the Buyer's delivery team are responsible for implementing the change where appropriate and ensuring it goes through the standard release processes.	The Supplier will support the Buyer where appropriate to deliver the associated Level 2 Services.
10.6	Design Changes – If an incident highlights an issue in the original design, the Buyer's architecture team will need to make a design decision on any changes that needs to be made to the design and inform Potential Provider and product teams.	Accepted.

10.7	Work Instructions – If the problem persists work instructions will need to be created collaboratively with the Buyer's delivery teams in line with the shift left approach, to prevent further incidents.	Accepted.

10.8	As part of regular monitoring of the system, The Supplier is responsible for raising any issues they see in production, pre-production (ESIT), training environments.	Accepted.
10.9	The Supplier will be assigned incidents for investigation via the Buyer toolsets. The Supplier must ensure the ticket is updated and closed once a resolution is accepted by The Buyer.	Accepted.
10.10	The Supplier will provide support to CtB Product Family as per the working hours agreed. All incident start and end times must be recorded.	Accepted.
10.11	The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration	Accepted.
11.1	As a requirement of the CCS Technology Services 3 Framework RM6100, The Supplier will need to provide an outline plan in their bid response.	Accepted.
11.2	Post Contract award The Supplier must include a full implementation plan consisting of a schedule of works, costs, deliverables and acceptance criteria	The Supplier will provide a detailed Implementation Plan within 20 working days of transition commencement (as per Schedule 1). The Supplier will provide a working draft within 2 weeks of commencement of Contract.
12.1	Reporting requirements will be captured in the Governance Schedule under Transparency Reporting, and these will be defined and agreed during engrossment.	Accepted.

12.2	Operational reporting and associated management processes such as RAID etc will be defined and agreed post engrossment.	Buyer to provide more information on the operational reporting requirements during Mobilisation / Transition Period. The Supplier accepts this requirement to perform operational reporting.
14.1	The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.	Accepted.
14.2	They should present new ways of working to the Buyer during monthly Contract review meetings.	Accepted.
14.3	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	Accepted.
15.1	The Buyer 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 will ensure throughout the duration of the Contract you will support in-work progression to help people, including those from disadvantaged or minority groups, to move into higher paid work by developing new skills relevant to the Contract.	Accepted in line with the obligations within T5 of the ITT Response.
18.1	The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service. Supplier shall manage seasonal variances effectively including legislative changes, etc	Subject to the Services scope defined in the Order Form.

18.2	The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.	Accepted.

18.3	The Supplier shall ensure that their staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.	Accepted.
19	The Service Hours for Production/ESIT environments: 24 hours	Accepted.
19	The Service Hours for Security Incident: 24 hours	Accepted.
19	The Service Hours for Training Environment: Mon to Sun 08002000, incl public holidays	Accepted.

19.1	The Service Levels tables below are for Production/ESIT environments: P1 means an Incident: a) that results in a complete or substantial loss of the Service; or (b) that results in an essential part of the Service being unusable for all End Users; or (c) that results in all End Users being unable to access the Service. Response Target 100% <= 15 mins Resolution Target 100% <= 4 hours P2 means an Incident: (a) where the Service is materially adversely affected, but can be circumvented; or (b) where the Service remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of End Users is unable to access the Service; or certain material aspects of the Service.	These Service Levels will apply to Production / ESIT environments as per ITT.

	Response Target: 100% <= 30 mins Resolution Target: 100% <= 8 hours P3 means an Incident: (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 (b) affecting a single or small group of End Users. Response Target: 100% <= 24 hours Resolution Target: 95% <= 2 Working Days, 100% <= 5 Working Days P4 means an Incident: (a) that results in little or no material impact on the Service or the Customer's business; or (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. Response Target: 100% <= 48 hours Resolution Target: 95% <= 3 working days, 100% < 5 working days	

19.2	The following table is for nonproduction environments which include Training Environment P1 - N/A P2 means an Incident: (a) that results in a complete or substantial loss of the Environment; or	Accepted.

	(b) that results in an essential part of the Environment being unusable for all Users; or (c) that results in all Users being unable to access the Environment (d) impacts the ability to deploy releases or fixes into Production (e) impacts the velocity of the delivery teams Resolution Target: 100% 8 hours (within Operating Hours) P3 means an Incident: (a) where the Environment is materially adversely affected, but can be circumvented; or (b) where the Environment remains operable, but certain material aspects of the Service are disabled; or (c) where a large group of Users are unable to access the Environment; or certain material aspects of the Service Resolution Target: 100% within 3 working days P4 means an Incident: (a) that results in a minimal impact for the Service where noncritical functions or procedures are down, unusable, or difficult to use; or (b) affecting a single or small group of End Users. Resolution Target: 100% within 5 working days	
19.3	The following Service levels are for Security incident Management P1 means an Incident:	Accepted.

	Any Incident which may cause the degradation of vital service for a large number of users, in-	

	volve a serious breach of network security, affect mission critical equipment or services or damage public confidence in the Government. Response Target: 15 minutes Resolution Target: 100% <= 4 hours P2 means an Incident: Incidents which are not Critical, and which may impact a smaller group of Users, disrupt non-essential services, breach network security policy or affect the reputation of Government bodies and services. Response Target: 30 minutes Resolution Target: 100% <= 8 hours P3 means an Incident: Incidents which are neither Critical, nor High and which can be handled by local IT and security offices. These Incidents do not typically impact IT services and include examples such as unsuccessful denial-of service attacks or the majority of network monitoring alerts. Response Target: 24 hours Resolution Target: 95% <= 2 Working Days, 100% <= 5 Working Days P4 means an Incident: Incidents, which are not Critical, High nor Medium and are in general considered to be part of normal IT support operations. These incidents would include receipt of an isolated SPAM or anti-virus alert, minor computer hardware failure, loss of net-	

	work connectivity to a peripheral device or loss of access to an external, non-essential service. Response Target: 48 hours Resolution Target: 95% <= 3 working days, 100% < 5 working days	
19.4	The following Service levels apply for CTB Service request/Account Management: - Account Creation - 09:0017:00, Monday to Friday excl. PH's - 5 working days - Amend (role change) - 09:0017:00, Monday to Friday excl. PH's - 5 working days - Disable/Re-enable (role change, name change, update SC expiry date) - 09:00-17:00, Monday to Friday excl. PH's - 5 working days	Accepted.
19.4	The following Service levels apply for CTB Service request/Account Management: - Account Unlock - 24/7, 4 hours	Accepted.

19.5	The Buyer will measure the quality of the Supplier's delivery by adherence to the following KPI's: KPI - Service Area - KPI/SLA description 1 - Incident Management - P1 Incident Task resolution 2 - Incident Management - P2 Incident Task resolution 3 Incident Management P3 Incident Task resolution 4 Incident Management P4 Incident Task resolution	Accepted.

	5 Service Request fulfilment Service Request Task fulfilment 6 Operational Change Management Operational Change Assessment 7 Operational Change Management Successful Operational Changes 8 Problem Management Problem Root Cause Analysis 9 Incident Management P1 Incident Task resolution 10 Incident Management P1 Incident Task response 11 Incident Management P2 Incident Task resolution 12 Incident Management P2 Incident Task response 13 Incident Management P3 Incident Task resolution 14 Incident Management P3 Incident Task response 15 Incident Management P4 Incident Task resolution 16 Incident Management P4 Incident Task response 17 Service Request fulfilment Service Request Task fulfilment 18 Operational Change Management Operational Change Assessment	

	19 Operational Change Management Successful Operational Changes	

	20 Problem Management Problem Root Cause Analysis	
19.6	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.	Out of scope for transition. The incentive process and measurement will be agreed as part of conformance.
19.7	An exit strategy for poor performance will be drafted and defined during the first 6 months of Contract Commencement	Accepted.
20.1	CtB is the digital “front door” into the UK at the border and as such is a critical service and must be available 24 hours a day 365 days of the year meeting at minimum 99.93% service availability.	Accepted.
20.2	Availability, capacity and performance management procedures ensure that the cost-justifiable IT capacity is in place, and the solutions are meeting the availability and performance needs of the Buyer.	Accepted.
20.3	This is delivered within the current solutions and considered as forecasts and part of the deliverable features for future business needs	Accepted.
21.1	The Supplier is required to deliver a HOD aligned, and collaborative capability providing both proactive and reactive problem management support under the governance of the HO HOD’s Problem Management operating model.	Accepted.
21.2	The Supplier will:	Accepted.

21.2.1	Perform a Root Cause Analysis (RCA) and collaborating with other teams during this process resolve the root cause	Accepted.

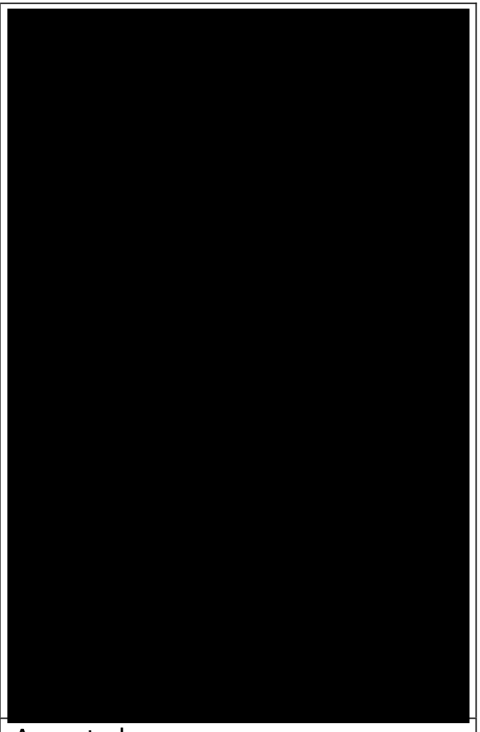
21.2.2	Develop workarounds until the fix can be released to production	This requirement will be owned by Level 3 and the Supplier will collaborate with Level 3 to develop an agreed workaround and fix.
21.3	The Supplier will adopt a proactive approach to Problem Management, seeking to resolve known errors and eliminate the root causes of incidents.	Accepted.
21.4	Report the success of proactive problem management through enhanced reporting in the monthly service performance pack, reviewed at the monthly Service Review Board.	Accepted.
22.1	As part of the support activities, The Supplier will work with HOD, product delivery teams, the operational support teams, site reliability engineering and service transition teams to ensure that appropriate and necessary thresholds, triggers, and alerts have been implemented as part of the solution within each feature's release.	The Supplier will work collaboratively with all the suppliers within the ecosystem to ensure all changes driven by the suppliers have appropriate thresholds, triggers and alerts before they are deployed into Production.
22.2	The Supplier will work with product delivery teams to ensure that monitoring alerts are captured appropriately and disseminated to the required tools. All alerts will be fully documented with their resolution scripts provided by the product delivery teams, and these will be provided to the Supplier.	The Supplier will work collaboratively with all the suppliers within the ecosystem to ensure all changes driven by the suppliers have appropriate alert monitoring before they are deployed into Production.

22.3	Further integration of where monitoring and alerts appear may be required if tooling changes or requirements change	The Supplier will work collaboratively with all the suppliers in the ecosystem to ensure any changes to the tooling or requirements are reflected in the new tooling before the change is deployed into Production.
23.1	In the day-to-day systems management and operational support of the CtB Product Family, the Supplier shall work in a Level 2 support capacity in line with requirements assigned to them by the relevant teams	Accepted.

24.1	The Supplier shall observe the below key principles to support the Product Family Business Continuity and Disaster Recovery (BCDR) plan as and when required.	Accepted.
24.2	The Supplier shall include plans for relocation of Potential Provider personnel in the event of a disaster at their work location in their BCDR Plan.	[redacted]
24.3	The Buyer shall review the Supplier BCDR plans, and provisions will be required where the Supplier co locates in Buyer premises as part of service delivery or invoked BCDR	Accepted.
25.1	The Supplier will deliver all changes into the Live Services in accordance with HOD's Change Management operating model. There is a responsibility for the delivery teams to understand if releases are Impacting or nonimpacting, as defined below:	Accepted.

25.1.1	Impacting releases: Releases that cause down time, or impact other services and the way they work, such as new calls or added volumes. Required lead time of 5 working days.	Accepted.
25.1.2	Non-impacting releases: Selfcontained with a service and tend to be rolling, no down time deployments. Required lead time 1 working day.	Accepted.
25.2	Release delivers enhancements, maintenance, and new services to the product family.	Accepted.
25.3	In accordance with the Change and Release processes, as appropriate the Supplier will deploy all approved and tested releases or action the deployment schedule as part of a continuous	Accepted.

	delivery approach through agreed pipeline release cycles.	
25.4	The Supplier will be required to work with the HOD Change & Release Management Team to impact assess all the required releases and changes. The HOD Change & Release Team will confirm the approvals prior to release and deployment.	Accepted.
25.5	The Supplier shall comply with the Buyer's Relevant Change Management processes	Accepted.

26.1	The Supplier shall provide application systems and associated platform support, ensuring endto-end service coverage for the CtB Product Family, including infrastructure components as required.	
27.1	The Supplier shall deliver their services in accordance with Home Office HOD's security policies and security management processes and procedures.	Accepted.
27.2	The Supplier shall ensure that all systems are operated in such a manner to support compliance with HMG Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework	Accepted.
27.3	Where appropriate, The Supplier will be required to hold Cyber Essentials, ISO27001 or an equivalent accreditation as per the terms of the CCS Technology Services 3 Framework RM6100	Accepted.

28.1	The Supplier shall:	Accepted.
28.1.1	Put in place processes and procedures that enable accurate and timely service delivery and performance measurement.	Accepted.

28.1.2	Measure and report service level performance results as documented and agreed to in contract documents.	Accepted.
28.1.3	Conduct service measurement in an agreed manner that is reproducible, auditable, and compliant with the signed contract documents.	Accepted.
28.1.4	Schedule and participate in the monthly and ad-hoc service reviews.	Accepted.
28.1.5	Submit performance results, data files, and supporting documentation for service level review reporting (and related activities) on time, as specified in signed contract documents, or in agreed implementation timetables or reporting schedules.	Accepted.
28.1.6	Provide the following deliverables as a minimum: metric results, supporting data files, root cause analysis, service corrective actions, Service Corrective Action Plans, assessment responses, remediation plans, and improvement plans.	Accepted.
28.1.7	Actively participate in the service review and operational meetings.	Accepted.
28.1.8	Engage cooperatively and proactively in remediation or improvement activities for the entire end to end services in scope of the Contract, including underperforming components which may be in scope for improvement.	Accepted.

29.1	The Supplier shall work collaboratively and dynamically, to ensure that knowledge is shared and transferred effectively within the CtB Product Family systems and support teams, and its designated users, in accordance with HOD's Knowledge Management Operating Model.	Accepted.
29.2	The Supplier shall:	Accepted.
29.2.1	Support the mutual exchange of knowledge and skills. progressing towards becoming a product driven organisation, encouraging knowledge and skills transfer from skilled suppliers to Civil Servants and equally in return. This includes methods, tools, industry good practice, and learned experiences.	Accepted.
29.2.2	Collaborate in the development of materials for self-learn, that may include QRGs, short video or other appropriate materials to facilitate accelerated knowledge transfer, support service transition, and all other ongoing service operations,	Accepted.
29.3	Examples of this include:	Accepted.
29.3.1	Technical Specifications	Accepted.
29.3.2	Work Instructions for incidents, monitoring and alerting, any known risks, or issues.	Accepted.
29.3.3	Production of user guides, knowledge articles, some technical specification definitions	Accepted.

29.3.4	Working collaboratively with other suppliers and Civil Servants across multidisciplinary teams, to achieve the organisational goals.	Accepted.
29.3.5	Providing staff who will be integrated into teams to share, develop, and increase domain knowledge.	Accepted.

29.3.6	Ensuring a robust handover process is mutually agreed, to limit skill and knowledge disruption, once resources progress and move on, as suppliers manage them.	Accepted.
30.1	The CtB Product Family consists of several multi-disciplinary delivery teams working across one or more of the services described earlier. The Supplier team will complement the multi-disciplinary delivery teams by providing suitably skilled and experienced resources.	Accepted.
30.2	The Supplier shall:	Accepted.
30.2.1	Support the requirement of teams to flex resources up or down over the course of the contract and in line with the business needs, subject to change control.	Accepted.
30.2.2	Ensure that there are sufficient resources in place to meet the business's need, as defined in the SLA's.	Accepted, as necessary to deliver associated Level 2 Services.
30.2.3	Ensure there is sufficient resources to provide eyes on glass support and troubleshooting.	Accepted.
31.1	The Supplier shall:	Accepted.

31.1.1	Adhere to Civil Service values	Accepted.
31.1.2	Make decisions transparent and collaborative	Accepted.
31.1.3	Have a no-blame culture and encourage people to learn from their mistakes	Accepted.
31.1.4	Work well in a team within our organisation	Accepted.
31.1.5	Mentor members of the team	Accepted.
31.1.6	Have a flexible attitude and temperament	Accepted.
31.1.7	Share knowledge and experience with other team members	Accepted.

31.1.8	Communicate with openness and clarity to technical and nontechnical stakeholders	Accepted.
31.1.9	Take responsibility for the quality of their work	Accepted.
32.1	All work deemed out of scope of the core requirements will be subject to the strategic demand forum and will be agreed by way of Statement of Works. We require The Supplier to provide the CtB Product Family deliverables through an agreed and written Statement of Work (SOW). These SoWs will outline the expected outcomes for each period and provide itemised costs for the Buyer. There is a general expectation that outcomes will align with product roadmap commitments. The Supplier shall assess, plan, and deliver the services required in each Statement of Work.	Accepted.

32.2	Statements of Work may cover specific delivery led periods, the duration can vary according to the predictability of the roadmap, the need for a quick response to urgent Government initiatives, and for other factors. There may be multiple overlapping Statements of Work, each covering a specific workstream or function within The Supplier organisation (as an example, change delivery and Level 3 support are often covered in separate Statements of Work to support the Buyer's financial reconciliation processes). Statements of Work are usually agreed per product, e.g., there are separate SOWs covering Helios, Border Crossing (BX), BX Tools. However, The Supplier is encouraged	Accepted.

	to recommend simple and effective methods of documenting outcomes and costs in SOWs to minimise paperwork and ensure simple and effective coverage. SOW proformas will be provided as part of the final Contract.	
33.1	In addition to the governance and reporting processes outlined in the call-off terms, the Buyer requires that Potential Providers submit management information in the form of monthly balanced scorecard status reports and present at a monthly meeting.	Accepted.

33.2	Further guidance on the process will be provided as and when required. The balanced scorecard approach helps drive consistency of performance measurement across The Supplier base. The Buyer and The Supplier take a collaborative approach; Buyer's assessors across the CtB Product Family who interface with Potential Providers to give feedback in a prescribed template to the Commercial Team. Potential Provider's will also be responsible for self-certifying their performance against the scorecard and provide this to the Commercial Team in a monthly balanced scorecard report.	Accepted.
33.3	The established scorecard KPI's will measure Potential Provider's performance monthly. The Buyer will provide feedback against service levels and KPI's to The Supplier each month.	Accepted.
33.4	An example of the balanced scorecard status report template to be used by The Supplier	Accepted.

	is provided in. Such reports should include, as a minimum:	
33.4.1	Delivery performance against requirements	Accepted.
33.4.2	Spend to date against requirements (Financial model)	Accepted.
33.4.3	Identification of customer dependencies	Accepted.
33.4.4	Highlighting any potential delivery issues	Accepted.

33.4.5	Adherence to the incentive scheme and associated behavioural metric	Out of scope for Transition. The incentive process and measurement will be agreed as part of conformance. The Buyer accepts it will not unreasonably withhold the 1% incentive from The Supplier.
34.1	The Supplier will deliver the requirements in this document in compliance to in-scope Services detailed in this document, with changes required post award subject to commercial change mechanisms and agreement between all Parties in accordance with, but not limited to the procedures outlined in Schedule 5 of the Call-off Terms and the strategic demand forum.	Accepted.
35.1	On request the Supplier shall provide to the Buyer an analysis of the volumetrics (or other measure(s) of usage) of the Services to the extent reasonably necessary to enable the Buyer to plan migration of such workload to a Replacement Supplier provided always that this analysis involves providing performance data already delivered to the Buyer as part of the performance monitoring regime.	Accepted.
35.2	The Supplier shall provide such information as the Buyer reasonably considers necessary for the actual Replacement Supplier, or any potential Replacement Suppliers during any reprocurement process, to define	Accepted.

	the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.	
36.1	On request the Supplier shall provide the Buyer an analysis of the volumetrics (or other measure(s) of usage) of the Services to the extent reasonably necessary to enable Transfer of Service Management Process.	Accepted.
36.2	Three months prior to expiry or within two (2) weeks' notice of termination of the Contract, The Supplier shall deliver to the Buyer:	Accepted.
36.3	A plan for the handover and continuous delivery of the CtB Product Family systems and support service function and allocate the required resources	Accepted.
36.4	Full and up-to–date data, covering historical and outstanding CtB Product Family system and service tickets including, but not limited to:	Accepted.
36.4.1	Local Continuity Plans	Accepted.
36.4.2	Operating levels	Accepted.
36.4.3	Technical requirements to provide support	Accepted.
36.4.4	Early life support dashboard, detail	Accepted.
36.4.5	BAU dashboard detail	Accepted.
36.4.6	Service Operations data and operating processes	Accepted.
36.4.7	BAU Work Instructions	Accepted.

36.4.8	Access Requirements	Accepted.
36.4.9	Service Catalogue	Accepted.
36.4.10	Service Level reporting data	Accepted.

36.4.11	Buyer's Customer contact details	Accepted.
36.4.12	Monitoring software tools and configuration	Accepted. The Supplier will be using the Buyer's tooling.
37.1	In accordance with the directives across Government, The Supplier shall be required to read and understand the following policies and standards:	Accepted.
37.1.1	The review and adoption of current processes, Policies & Standards with introduction of governance mechanisms as required	Accepted.
37.1.2	The BCP/DR methodology will be based on best practice guidelines within the BS 25999 Business Continuity Management standard	Accepted. The Supplier does not hold BS 25999 however is compliant with ISO 22301 which has succeeded it.
37.2	The Supplier confirms that it is familiar with, and has sufficient competency in supporting and operating services built or managed using:	Accepted.
37.2.1	Flexible development methodologies and continuous delivery	Accepted.
37.2.2	Continuous integration and build automation	Accepted.
37.2.3	Fully proficient with ITIL capabilities and drive best practice	Accepted.

37.2.4	The Supplier confirms that ownership of all intellectual property in any deliverables is to belong to the Buyer.	Accepted.
38.1	The Supplier will be required to hold Cyber Essentials Plus and ISO27001 or an equivalent accreditation as per the terms of the CCS Technology Services 3 Framework RM6100. The Buyer will require a copy of the accreditation certificate prior to start of mobilisation of the services.	Accepted.

38.2	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 may be a requirement for further clearance to be held NPPV3. Please see United Kingdom Security Vetting - GOV.UK (www.gov.uk) for further details.	Accepted.
38.3	Potential Providers 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.	Accepted.

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

38.8	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	Accepted.
39.1	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's ICT services.	Accepted.
39.2	The Supplier shall be ISO/IEC 27001 and Cyber Essential Plus accredited. The Supplier shall ensure that they have active ISO/IEC 27001 and Cyber Essentials Plus accreditation throughout the duration of the Contract for any of their locations used to provide any Services in scope of this Contract.	Accepted.
39.3	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 the Buyer's additional onboarding	Accepted.

	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 caseby-case basis.	
39.4	Potential Provider 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 were agreed with the Buyer's in writing.	Accepted.
39.5	The Suppliers staff 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 hold a valid BPSS check as a minimum which includes; identity, unspent criminal convictions and right to work.	Accepted.
39.6	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/	Accepted.

39.7	The Supplier shall ensure that Potential Provider 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	Accepted.

	and also undergo any required Buyer led training. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.	
39.8	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.	The Supplier will notify the Buyer without undue delay of any cyber attack that: a) directly impacts the CtB Level 2 Service, Buyer data, or systems used in delivery of CtB Level 2; b) affects Supplier operations where there is a reasonable likelihood of impact to the CtB Level 2 Service or Buyer data; and/or c) affects the Supplier and becomes the subject of public disclosure or regulatory notification. For incidents under (a) the Supplier shall provide full details of impact and remediation. For incidents under (b) and (c), the Supplier will provide all information reasonably necessary for the Buyer to assess the risk to the Services, provided that such disclosure does not require the Supplier to breach applicable law or any existing contractual obligations to third parties.
39.9	The Supplier shall report any non-compliance with the Buyer's security policies and procedures appropriately.	Accepted.

39.10	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.	Accepted.
39.11	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	Accepted.
	understood and adhered to in order to manage risk effectively.	
39.12	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.	Accepted.

39.13	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.	Accepted.
39.14	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.	Accepted.
39.15	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.	Accepted.
39.16	The Supplier shall ensure that all National Cyber Security Centre (NCSC) good practice, guidelines or advisories are followed.	Accepted.

	Where there are none relevant best industry practises should be followed.	

39.17	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	Accepted.
39.18	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.	Accepted.
39.19	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.	Accepted.
39.20	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.	Accepted.
39.21	The Supplier shall provide support via technical means from agreed UK based locations aligned to security and policy requirements. The Supplier will	Accepted.

	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.	
39.22	The Buyer data shall not be subject to offshoring arrangements.	Accepted.
39.23	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.	Accepted.
39.24	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.	Accepted.

39.25	The Supplier shall ensure that Potential Provider 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 Potential Provider 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	Accepted.
42	The system should ensure information is encrypted in transit on	Accepted. This requirement is limited to data held or stored on systems owned by the Supplier.

	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	
43	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	Accepted.

44	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 Buyer authorised devices/locations and be requested or authorised for timebound durations	Accepted.
45	Security logging must be enabled to support incident investigations, forensics and provide continuous security monitoring to detect suspicious user, ad-	Accepted.

	ministrator, 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	

46	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 IBM corporate devices are not in scope for this requirement.	Data backup is a Buyer responsibility. Level 2 shall support the Buyer with executing Data recovery policy/processes.
48	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	The Supplier will cover within the scope of Level 2 monthly reporting and attend SWGs if required.
49.2	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.	Accepted.
49.3	All changes/releases deployed into the pre-production/production environments must be controlled through a robust change management process.	Accepted.
49.4	A process should exist for controlling the regular deployment of patches into the productive	Accepted.
	environments in a timely manner.	

49.5	All security incidents must be recorded, tracked through to closure and communicated to stakeholder following a security incident Management Process.	Accepted.
49.6	The system must have a business continuity plan which is periodically tested to ensure the system can be recovered following a major incident	Accepted.
54.1	The Supplier must ensure that all systems are operated in such a manner that;	Accepted.
54.2	The CtB Products shall be able to monitor the operational health and usage of the applications and services used by the CtB Product Family.	Accepted. For clarity, Level 3 will provide monitoring information, Level 2 will not accept anything into Production, Training and ESIT that cannot be monitored by Level 2.
54.3	The Supplier must comply with the Buyer's policies and the EU Directive on PNR Data and any applicable legislation.	Accepted, as necessary to deliver associated Level 2 Services.
54.8	Level 2 is required to maintain an Level 2 support risk register and input to the Buyer's risk register	Accepted.
54.10	Unless deemed an emergency scenario The Supplier will be required to support any downtime for the CTB capability within agreed change windows	Accepted. It is jointly agreed that the Release team will schedule the appropriate time and Level 2 will then deploy as required.
55.1	The Supplier shall ensure that all tests are included with the correlated code and configuration changes within the source and version control process.	Level 2 testing scope will be limited to testing deployment scripts and work instructions provided by Level 3. Post deployment test would be for Level 2 to complete unless instructed otherwise. All remaining Test activity to be led by Level 3 and QAT.

55.2	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.	Level 2 testing scope will be limited to testing deployment scripts and work instructions provided by Level 3 if required. All remaining Test activity to be led by Level 3 and QAT.

55.3	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.	Level 2 testing scope will be limited to testing deployment scripts and work instructions as defined by the L3 and QAT teams.
55.4	The Supplier shall ensure that release performance tests are automated to verify that no unacceptable service degradations are released.	Level 2 testing scope will be limited to testing deployment scripts and work instructions as defined by the L3 and QAT teams.
55.5	The Supplier shall adopt and subscribe to the Buyer's security testing processes and adopt a shift left approach in the delivery pipeline.	Level 2 testing scope will be limited to testing deployment scripts and work instructions as defined by the L3 and QAT teams
55.6	The Supplier shall work with QAT as required to ensure that code, test and requirement coverage metrics are agreed and measured per component for each release.	Accepted.
55.7	The Supplier shall ensure that no component is delivered that exceeds the agreed defect threshold and criteria for the related test phase.	Level 2 testing scope will be limited to testing deployment scripts and work instructions provided by Level 3. All remaining Test activity to be led by Level 3 and QAT.

55.8	The Supplier shall utilise the Buyer's defect classification model and record all related defect information within the Buyer's JIRA/ServiceNow instance. Where the security classification of the defect prevents the utilisation of JIRA / ServiceNow the Buyer will agree an alternate method with The Supplier.	This requirement covers BAU and test environment. Level 2 maybe required to raise a ticket for items identified.
55.9	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 con-	Accepted. For clarity, Level 2 testing scope will be limited to testing deployment scripts and work instructions as defined by the L3 and QAT teams.

	tent of said artifacts with be collaboratively agreed with the Buyer's test assurance team.	
55.10	The Supplier shall follow the Buyer's overarching test strategy and collaborate on any changes or enhancements required to support the product.	Accepted.
55.11	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	Accepted. Level 2 is expected to contribute to the test strategy and RACI.
56.1	Invoices for payment should be submitted monthly in arrears.	Accepted.
56.2	Payment will only be processed on receipt of a valid invoice containing the relevant purchase orders details.	Accepted.

Crown Commercial Service

56.3	Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.	Accepted.
56.4	Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.	Accepted.
56.5	Invoices should be submitted to: HOSuppli-erInvoices@homeoffice.gov.uk	Accepted.
57.1	The Supplier will be required to attend regular contract management meetings (monthly) where the following areas will be discussed:	Accepted.
57.1.1	Review and agreement of works to be completed under a statement of works	Accepted.
57.1.2	Supplier performance/KPI review	Accepted.
57.1.3	Review of delivery against key miles stones	There are no Key milestones therefore this requirement is out of scope. Level 2 Services will be subject to a monthly billing schedule, invoiced 30 days in arrears.
57.1.4	Risk and Issues	Accepted.
57.1.5	Please note this list is not exhaustive.	Accepted.
57.2	The Supplier must ensure their attendance in relation to Balanced Scorecard contract review meetings every month and ensure their attendance at ad-hoc and planned technical/delivery check-in meetings.	Accepted.
57.3	Attendance at Contract Review meetings shall be at The Supplier's own expense.	Accepted.

58.1	The Services may be delivered to any Home Office locations, as agreed with the Buyer. Supplier resources working at these locations will need to ensure they comply with guidance provided by the MBTP Security Team.	Accepted.
58.2	Access to relevant Home Office Systems may be granted following appropriate completion of security checks and end user device agreement.	Accepted.
58.3	The Supplier shall provide onsite support with access to a secure room.	[redacted]
58.4	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 24/7 to support incident management and associated processes.	Accepted for travel to Buyer locations listed in the SAL.
59.1	All devices must comply with the MBTP End User Device Agreement.	Accepted.
59.2	Devices must be corporate issued and well managed.	Accepted.
59.3	Devices will be validated to ensure EUDA compliance by the MBTP Cyber Team. Periodic checks throughout the contract life will also take place.	Accepted.
59.4	Personal devices are NOT permitted to be used for MBTP projects	Accepted.
60.1	The Supplier will be required to work outside the standard operational day e.g. monitoring of service and a failure of service.	Accepted.

60.2	Provision of an Out of Hours (OOH) service, managing agreed incidents outside of core service hours.	Accepted.
60.3	The Supplier will provide Out of Hours support for the products when required.	Accepted.
60.4	Core support hours are 0800 to 20:00 (including Bank Holidays) Support will be required 365 days	Accepted.
60.5	Appropriately skilled resources will be available 24/7, 365 Days, to respond to any incidents.	Accepted.
60.6	A rate as agreed and in accordance with the rates covered (HO Digital Service Rate Card) will be applied if required.	Accepted.
61	Please refer to clause 58.4	Accepted.
62	New requirement added after ITT. The Supplier shall actively collaborate with the Service Integrator to support the delivery of a seamless end-to-end support for the CtB Product Family	Accepted within the scope of the Level 2 Services and in line with reasonable requests subject to the Collaboration Agreement.

OUT OF SCOPE Following engrossment, these requirements though originally included in the ITT issued, the Buyer agreed to de-scope them from the Level 2 support provision of the Supplier.

Table 4: Out of Scope Requirements of the CTB Level 2 Service

Reqt ID	Requirement	Reason for removal

Crown Commercial Service

40.1	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 to minimise the risks of unauthorised/untested changes and prevents leaking of production information into the non-productive environments.	Requirement is not within the scope of Level 2.
40.2	Threat and vulnerability management - 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	Requirement is not within the scope of Level 2.
41.1	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.	Requirement is not within the scope of Level 2.
41.2	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	Requirement is not within the scope of Level 2.
47	The system should be resilient to single points of failure	Not within the scope of Level 2 on the basis that no Buyer data or documents will be stored outside of Home Office systems.
49.1	All system hardware/software assets and their configuration deployed in the production system must be managed in a CMDB.	Requirement is not within the scope of Level 2.
50	The Supplier will report, manage an actual or suspected breach of information security of the service in line with the Buyer's HOD policy	Requirement is not within the scope of Level 2.

51.1	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.	Requirement is not within the scope of Level 2.
51.2	This will include;	Requirement is not within the scope of Level 2.
51.3	Contributing to identifying the systems, Configuration Items, or other service Components that should be monitored and establishing the Security monitoring strategy.	Requirement is not within the scope of Level 2.
51.4	Implementing and maintaining Security monitoring, using SIEM monitoring tools where relevant.	Requirement is not within the scope of Level 2.
51.5	Establishing and maintaining thresholds and other criteria for determining security events and choosing criteria to define each type of event (informational, warning, or exception).	Requirement is not within the scope of Level 2.
51.6	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.	Requirement is not within the scope of Level 2.
51.7	Implementing processes required to operationalise the defined thresholds, criteria, and policies.	Requirement is not within the scope of Level 2.
51.8	Regular checks to ensure the Application has not breached or application not being attacked.	Requirement is not within the scope of Level 2.
52.1	The Supplier will utilise security tooling as stated by the Buyer which includes, but not limited to;	Requirement is not within the scope of Level 2.
52.2	SIEM Tools: Splunk	Requirement is not within the scope of Level 2.
52.3	Vulnerability scanning: Tenable.io, SonarCube, Trivy etc	Requirement is not within the scope of Level 2.
52.4	AV: MS Defender	Requirement is not within the scope of Level 2.

52.5	IAM :- RedHat SSO	Requirement is not within the scope of Level 2.
53	The Supplier shall work collaboratively with the MBTP cyber security architects to ensure any design is secure and uses the Secure by Design Principles	Requirement is not within the scope of Level 2.
54.4	The Supplier shall collaborate with the Buyer to establish cost monitoring processes and where appropriate cost controls for cloud capabilities within the product.	Requirement is not within the scope of Level 2.
54.5	The Supplier will be required to follow and support the Buyer architectural and design governance practices.	Requirement is not within the scope of Level 2.
54.6	The Supplier will be required to follow the Buyer's architectural and design standards.	Requirement is not within the scope of Level 2.
54.7	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 Appendix 4	Requirement is not within the scope of Level 2.
54.9	The Supplier will ensure that CtB products can be shut down and started independently of other Buyer products with zero data lost during controlled processes	Following engrossment , this requirement is deemed out of scope for Level 2 Support Requirement is not within the scope of Level 2.

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

Not applicable

Part B – Service Charges

- Invoices for payment should be submitted monthly in arrears.
- Invoices should only be raised as profiled below or agreed with the Buyer through the Buyers' Change Control process approval process.
- Payment will only be processed on receipt of a valid invoice containing the relevant purchase orders details.
- Any payment not previously profiled and agreed must be approved through the Buyer's Change Control process following satisfactory delivery of pre-agreed certified products and deliverables.
- Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
- Invoices should be submitted to [redacted]

Table 4: Payment Schedule

[redacted]

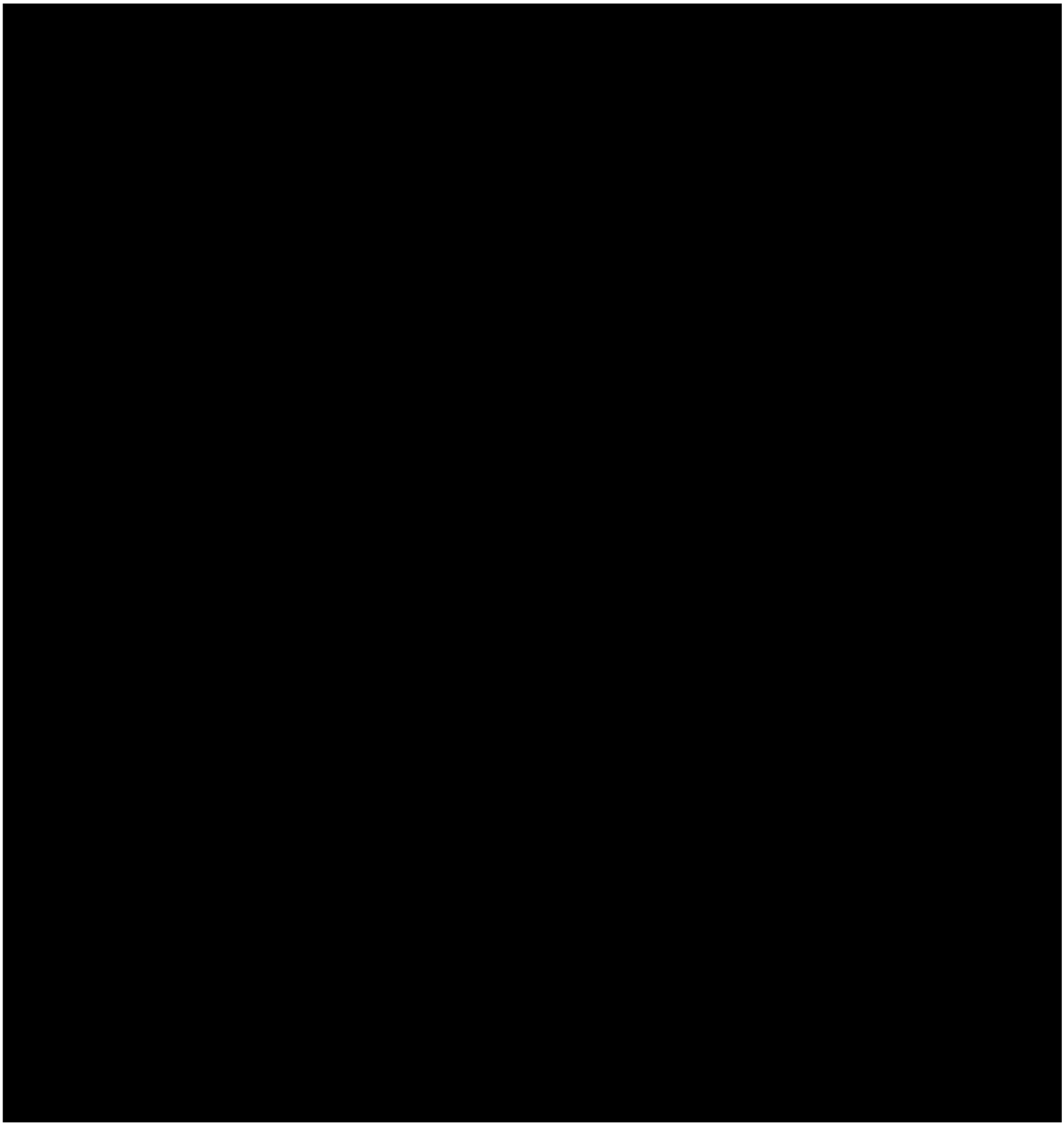
Crown
Commercial
Service

[redacted]

Crown
Commercial
Service

[redacted]

Crown Commercial Service



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

Crown Commercial Service

Staff Grade	Day Rate (£)
Not Applicable	

Crown Commercial Service

Part D – Risk Register

Risk Number	Risk Name	Description of Risk	Timing	Likelihood	Impact	Mitigation (Description)	Owner
1	Knowledge Transfer (KT)	There is a risk that Knowledge Transfer is not completed and therefore does not meet agreed criteria between both parties over the live Service due to a high dependency on the current incumbent supplier to ensure completion of knowledge transfer (KT) and transition activities within the required timescales .	KT Start	MEDIUM	HIGH 1. Quality of service may be impacted due to delays in incident resolution and fulfilment task completion. 2. The Buyer may need to relieve the Supplier of service credits until able to operate the service fully.	1. The Buyer shall ensure reasonable access to incumbent resources and documentation for the purpose of KT. 2. The incoming Supplier shall complete KT within agreed timelines, in collaboration with the incumbent. 3. Progress of KT will be tracked and reported to the Buyer on a weekly basis by the Supplier so that any progress and engagement issues can be addressed by the Buyer 4. Acceptance criteria will be defined and agreed at the outset to ensure Knowledge Transfer is completed fully prior to the Supplier taking over the Service. 5. The relief from Service Credit would be for a maximum of one quarter and reviewed monthly.	Buyer

Crown Commercial Service

2	[redacted]	[redacted]	Service Start	HIGH	Both Parties to agree cost impact on the Supplier contract and the Buyer on extending the services of the incumbent.	[redacted]	Buyer

Crown Commercial Service

Part E – Early Termination Fee(s)

Early termination fees do not apply.

Attachment 3 – Outline Implementation Plan

Dependencies will be identified during creation of the Detailed Transition Plan.

Table 5: Deliverables of the Transition Period

ID	Deliverable	Format	Due Date
DEL01	Detailed Implementation Plan	Spreadsheet	Draft provided within first two weeks of Commencement Date. Final version within 20 working days of Transition Commencement.

DEL02	Weekly Transition Status Report	PDF	Weekly throughout transition
DEL03	Capability Readiness Assessment	PDF	Prior to Service Readiness checkpoint before Service Go Live Date.
DEL04	Monthly Service Report Template	PDF	Prior to Service Go Live date
DEL05	Supplier BCDR Plan	PDF	Prior to Service Go Live date

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

Service Levels and Service Credits

The method for calculating Service Credits shall be agreed during the Mobilisation/Transition Period. Annual check points will be undertaken throughout the Contract lifecycle where the Service Levels and Service Credits of the following year will be reviewed.

Service Levels and Performance

The KPI table below is an indication of the Key Performance Indicators and metrics the Buyer proposes to measure the quality of the Supplier's delivery.

The Buyer will measure the quality of all the Supplier's delivery within the CtB ecosystem by adherence to the relevant KPI's for their Service scope. The appropriate KPIs for the CtB Level 2 Service will be agreed by the end of the Mobilisation/Transition Period.

Table 6 Key Performance Indicators

	KPI	ON TARGET
1	Use of tooling, adherence to WoW, standards	100%
2	Availability of requirement information through agreed tooling	100%
3	Transparency on ways of working	TBC
4	Service Request Fulfilment - Catalogue / request management	100%
5	Incident Management– Incident response	100%
6	Incident Management– Incident resolution	100%
7	Social Value	TBC
8	Change management – No unauthorised changes or failed changes due to the Supplier's fault	0%
9	Provision of management information	TBC

Service Levels	Service Credit for each Service Period

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Relief given through Mobilisation/Transition Period	Relief given through Mobilisation/ Transition Period	Relief given through Mobilisation/Transition Period	Relief given through Mobilisation/Transition Period	Relief given through Mobilisation/Transition Period

Service Credit Cap

Maximum service credit value will be capped at 8% in any one month. The Service Credit methodology and associated calculation approach will be agreed by both Parties during Service transition. Service Credits will not apply to the Service during the Mobilisation /Transition Period until both parties have agreed the approach in writing. Both parties have agreed that Service Credits will be applied on a tiered basis and shall be capped at a maximum 8% of the associated monthly Service Charge however the methodology for calculation would be agreed during Mobilisation/Transition Period.

Critical Service Level Failure

Exempt from Mobilisation/transition period.
Critical Service Level Failure shall be informed by the service and application contracts within the ecosystem. Critical metrics will be agreed by the end of the Mobilisation/Transition Period.

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

Part A – Key Supplier Personnel

The Supplier agrees to update the information of key roles and duration on 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.

Crown Commercial Service

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

Part B – Key Sub-Contractors

Key Subcontractor 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
Not Applicable				

Crown Commercial Service

Attachment 6 – Software

The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

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

Part A – Supplier Software

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
Not Applicable							

Part B – Third Party Software

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
Not Applicable							

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

Crown Commercial Service

PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term)	Credit Rating Threshold
[redacted]		

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

PART B – RATING AGENCIES

Dun & Bradstreet (D&B)

Attachment 8 – Governance

PART B – LONG FORM GOVERNANCE

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, will be agreed once the Mobilisation/Transition 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 Mobilisation/Transition the Parties will operate at a minimum the following two governance boards:

- 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.
- 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. Supplier will be required to attend regular Contract management meetings (monthly) where the following areas will be discussed;

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

    Supplier performance/KPI review

    Review of delivery against key milestones

    Risk and issues

    Please note this list is not exhaustive.

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

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.

[redacted]

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Attachment 9.

Description	Details

Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • Contact information for the Buyer's staff for the purpose of processing system access requests **The Supplier is Controller and the Authority is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with Clause 34.2 to 34.15 of the following Personal Data*:* • Personal details of the Supplier's and its subcontractors' staff as necessary for the Buyer to provide and maintain security clearance and administer site and system access necessary for the staff to perform their roles under the contract. **The Parties are Joint Controllers** The Parties acknowledge that they are not Joint Controllers for the purposes of the Data Protection Legislation in respect of: **The Parties are Independent Controllers of Personal Data**

	The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel, • Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under this Contract.
Duration of the processing	Data will be processed from Contract Signature to end of Contract in line with UK law and GDPR requirements. Duration of the contract is the 2nd February 2026 to 1st January 2031.
Nature and purposes of the processing	Buyer Data will be processed by the Supplier utilising Buyer tools in the provision of the Services. Data will be held on Buyer systems in line with the Home Office's Retention Policies.
Type of Personal Data	Supplier Staff data required for clearance and administration purposes: Name, Date of Birth, Address, Contact details. Buyer data required for the provision of the Services: Name, Username, phone details, work email addresses
Categories of Data Subject	Buyer, Buyer third party and Supplier Staff engaged in the provision of the Service.
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	Buyer, Buyer third party and Supplier Staff data will be removed from the system as part of the off-boarding process when they leave the team providing the service. In rare exceptions where data may be transferred to Supplier Systems or devices must be removed once the purpose for transferring such data is met. The Supplier must provide appropriate evidence that the data has been returned and/or destroyed, which shall be agreed with the Buyer before data is transferred. At the end of the Contract all staff data will be removed as part of the offboarding process, with only that data necessary for audit purposes retained.

Crown Commercial Service

Attachment 10 – Transparency Reports

Transparency Reports for the Implementation Period will be agreed once the Mobilisation/transition Period has concluded.

During the Mobilisation/Transition Period a weekly status report will be delivered in PowerPoint format to an agreed list of Buyer stakeholders in addition to the reports below.

Title	Content	Format	Frequency
Contract Monthly Performance Reports	Report on Performance	Pdf or MS Word	Monthly, one week before Performance Meeting
Charges	Charges breakdown incl. invoice numbers	Pdf or MS Excel	Monthly

Crown Commercial Service

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

CTB%20L2%20Support%20contract%20w

CTB%20L2%20support%20-%20Additional

Annex 2 – Call Off Special Terms

This Order Form amends the Framework Terms and Call-Off Terms as detailed below. The Special Terms contained in this Annex are incorporated into this Call-Off Contract:

Special Term 1: Clause 20 (Intellectual Property Rights) of the Call-Off Terms

New clause 20.7 inserted:

20.7 Nothing in this Contract (including Call-offs and Attachments) shall prevent the Supplier or its Subcontractors from using, for any purpose, that experience which is gained by Supplier Personnel or Sub-contractor in the provision of the Services; or prevent the Supplier from providing similar services and/or deliverables to others using the same or different staff.

Crown Commercial Service

Annex 3 – Security Aspects Letter

The Security Aspects Letter is attached below.

Home Office