



Crown
Commercial
Service

Bid Pack

Attachment 3 – Statement of Requirements

Contract Reference: CCZX22A03

FBIS Integration Layer

OFFICIAL

Attachment 3 – Statement of Requirements
Leah Emery
© Crown copyright 2018

V1.7 29th March 2022

CONTENTS

1.	PURPOSE.....	3
2.	BACKGROUND TO THE CONTRACTING AUTHORITY.....	3
3.	BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT	3
4.	DEFINITIONS.....	6
5.	SCOPE OF REQUIREMENT	6
6.	THE REQUIREMENT	7
7.	KEY MILESTONES AND DELIVERABLES	26
8.	MANAGEMENT INFORMATION/REPORTING	27
9.	VOLUMES.....	28
10.	CONTINUOUS IMPROVEMENT	28
11.	SUSTAINABILITY	30
12.	QUALITY	30
13.	PRICE	31
14.	STAFF AND CUSTOMER SERVICE	32
15.	SERVICE LEVELS AND PERFORMANCE	32
16.	SECURITY AND CONFIDENTIALITY REQUIREMENTS	34
17.	PAYMENT AND INVOICING	35
18.	CONTRACT MANAGEMENT	35
19.	LOCATION	35

OFFICIAL

1. PURPOSE

- 1.1 The Home Office is seeking a Supplier Partner to support delivery of the key objectives by providing capacity and capability to develop, maintain and iterate strategic digital products and services. This procurement sets out the requirements for a Supplier partner to work within the Migration and Borders Technology Portfolio on the FBIS Integration Layer product.
- 1.2 The FBIS Integration Layer plays a pivotal role in the Portfolio's technical landscape. FBIS Integration Layer delivers the integration between a messaging backbone on Kafka and downstream application services to enable an event-based architecture.
- 1.3 The FBIS Integration Layer plays a pivotal role in the Portfolio's technical landscape. FBIS Integration Layer delivers the integration between a messaging backbone on Kafka and downstream application services to enable an event-based architecture.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

- 2.1 The Home Office is a Department of the Government of the United Kingdom with responsibility for maintaining the security of the country and the safety of its citizens. The key priorities of the Department therefore include the reduction of crime, including cyber-crime and serious and organised crime, protecting vulnerable people and communities, reducing terrorism and delivering world-class public services.
- 2.2 Home Office Digital, Data and Technology (HO DDaT) is part of the Home Office Capabilities and Resources Directorate, providing the Department with the enabling technology to run its business and provide customer facing digital services. The Migration and Borders Technology Portfolio (MBTP) within Digital, Data and Technology includes the work to run and maintain immigration system technology and services, as well as deliver major Government programmes.
- 2.3 Migration and Borders Technology Portfolio is organised in a product-centric manner, with BAU and programme objectives met where possible via a set of digital products. The FBIS Integration Layer product is amongst those products.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

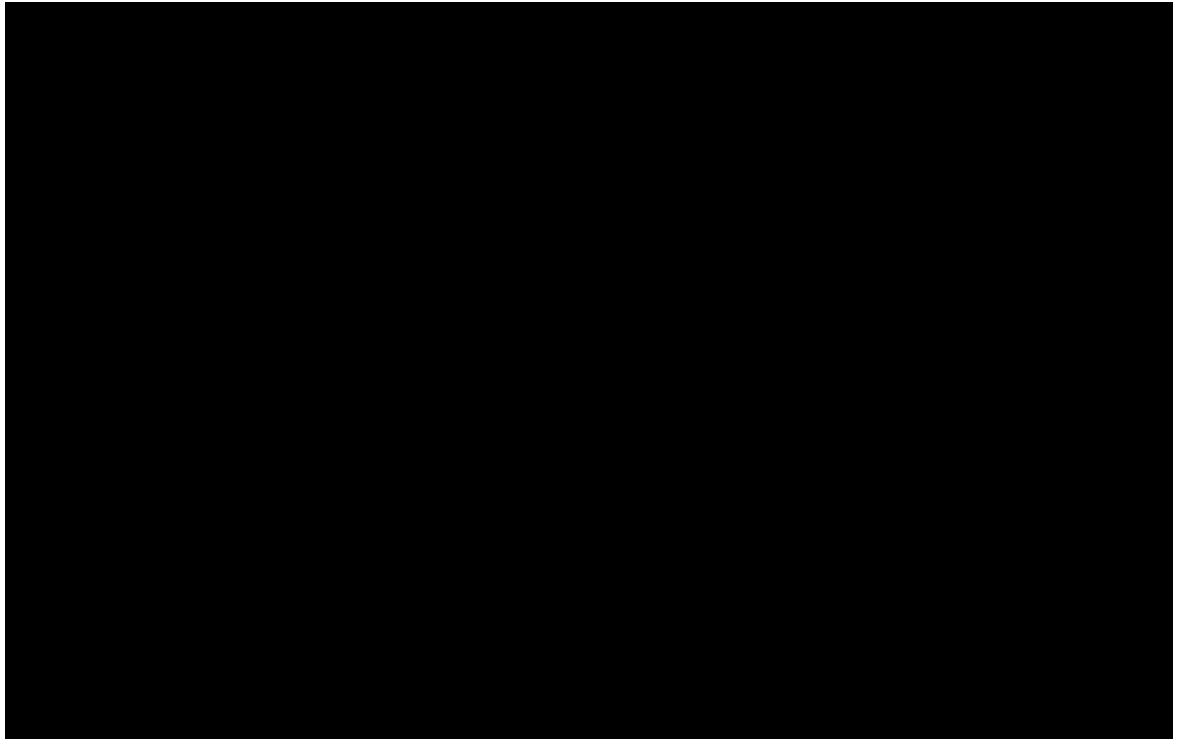
- 3.1 FBIS Integration Layer provides a series of components that integrate to Kafka via shared libraries. The components combined enable event-based integrations in line with the strategic architecture goals of Migration and Borders Technology Portfolio. Many of the integrations are critical to ensure business

OFFICIAL

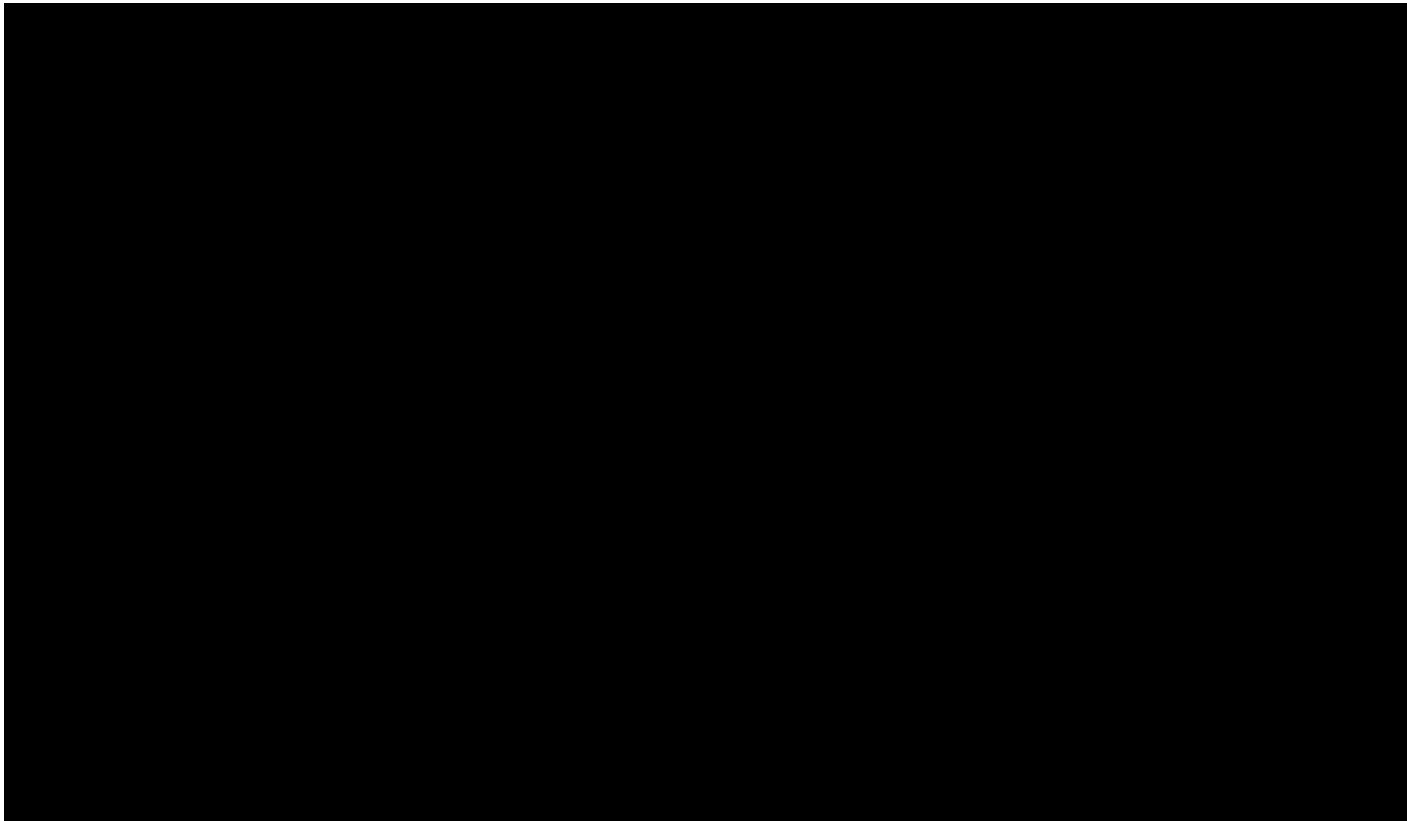
continuity of interactions from customers and as such need to be continuously available for 24 hours a day, 7 days a week, 365 days of the year.

- 3.2 Strategically the ownership of FBIS Integration Layer components will be transitioning to application services that are responsible for specific areas of the Migration and Borders Technology Portfolio technology landscape (e.g. case working, identity management, evidence management) and as such will need SME support from the FBIS Integration Layer team to enable this. This may involve the implementation of enhancements (either by creating tactical new components or making changes to existing components), decommissioning components or supporting the change of ownership to a different delivery team.
- 3.3 Home Office Digital, Data and Technology and the FBIS Integration Layer product employs Agile delivery methods, tailored to teams dependent on its maturity and the nature of the products and services in its remit. Multi-disciplinary teams within the organisation operate within a common set of architectural frameworks and a shared governance structure which connect them to wider organisational objectives. Consideration of how to prioritise and deliver the requirements for FBIS Integration Layer in line with the programme necessitates the need for a flexible approach in planning and delivery. Careful consideration of how to continue to build the FBIS Integration Layer product to best deliver re-use and generic capability is critical.
- 3.4 While more detailed prioritisation takes place within each Product Family and its teams, it is also consolidated across families to ensure that deliveries in one area do not jeopardise work in another and are co-ordinated where needed.
- 3.5 Work in the FBIS Integration Layer product roadmap include work from multiple products and will also include technical debt and work to implement the strategic architecture, as well as continuous improvement, technical debt and accessibility improvements.
- 3.6 Finally, Migration and Borders Technology Portfolio has a strategic aim to increase the number of civil servants in digital roles. Supplier partners will be expected to work alongside civil servant team members undertaking a wide variety of roles within typical multi-disciplinary teams. Over the life of the contract, the Supplier Partner will work with Migration and Borders Technology Portfolio to enable its self-sufficiency in most (if not all) digital roles and processes
- 3.7 Architecture overview

OFFICIAL



3.2 Technologies and Tooling



OFFICIAL

4. DEFINITIONS

Expression or Acronym	Definition
FIL	means FBIS Integration Layer
HOD	means Home Office Digital
DDaT	means Data and Technology
MBTP	means Migration and Borders Technology Portfolio – the technology teams responsible for delivering digital services to support migration and borders
BESS	means Business Event Streaming service – this is an MBTP application service built on Kafka
SME	means Subject Matter Expert – individuals who have detailed knowledge on a specific subject area

5. SCOPE OF REQUIREMENT

In Scope	Out of Scope
----------	--------------

OFFICIAL

Delivery effort costs. This is defined as the cost of staff directly engaged on the FIL product to deliver the service to the Authority.	Training and recruitment costs, including but not limited to; pre-employment check costs (e.g. completing SC questionnaire), recruitment agency fees.
	IT and office equipment (e.g. laptops, smartphones, desks, chairs etc), tooling and license.
	Company management or administration costs

6. THE REQUIREMENT

- 6.1 The term of this Call-Off Contract shall be three years from the Effective Date. The Authority shall include an additional two (2) optional twelve (12) month extension periods. Each extension period may last up to twelve months in duration. The right to exercise any of these extension periods shall be entirely at the Authority's discretion. Subject to the Authority's determination, the extension shall be implemented via the Change Control Procedure as detailed in the Call-Off Contract Schedule 5 (Change Control Procedure) Part B – Long Form Change Control Schedule.

Reference	Category	Requirement	Criticality
DEL01	Delivery	The Supplier will deliver the Product roadmap using a range of structured programme and project management methodologies, including Agile at scale and pace.	Must Have
DEL02	Delivery	The Supplier will plan with capacity for the team to deal with high priority ad hoc issues.	Must Have
DEL03	Delivery	The Supplier will utilise HO project delivery lifecycle methodology and toolset where required.	Must Have
DEL04	Delivery	The Supplier will collaborate with Portfolio Business Engagement leads/ Business and Technical Architects, and Analysts to complete early analysis of proposed improvements to develop business requirements.	Must Have

OFFICIAL

DEL05	Delivery	The Supplier will monitor and develop metrics to demonstrate team progress/ performance that will inform the project plans so outcomes/ milestones will be more predictable.	Must Have
DEL06	Delivery	The Supplier will develop and enhance team productivity through reviewing team metrics to identify improvements.	Must Have
DEL07	Delivery	The Supplier will proactively monitor dependencies, interdependencies within programmes or between related projects, risks and issues – with timely escalations when appropriate.	Must Have
DEL08	Delivery	The Supplier is expected to transition elements of the delivery to BAU live support teams. They will need to engage with DDaT Service Design and Transition and comply with the DDaT Service Design & Transition Governance and Process.	Must Have
DEL09	Delivery	The Supplier will be expected to train Civil Servants in line with any Service offering of training; this should include day to day tasks, tooling and integrations.	Must Have
DEL10	Delivery	The Supplier will deliver and manage several hosting environments to support the journey to live for FIL and its clients. The largest environment is a full- scale production environment which processes the FIL data collection.	Must Have
DEL11	Delivery	The Supplier will provide reporting as per the DDaT and programme level governance processes.	Must Have

OFFICIAL

DEL12	Delivery	The Supplier will provide and support access to near real-time information improving quality of decision-making processes.	Must have
DEL13	Delivery	The Supplier will increase business agility by enabling the introduction of new capabilities with minimal disruption to existing systems and services.	Must have
DEL14	Delivery	The Supplier will improve business ability to respond to spikes in service demand as required.	Must have
DEL15	Delivery	The Supplier is expected to deliver new functional changes requested by the business that require changes to core capability.	Must Have
COR01	Core	The Supplier shall continue development and support of the existing FIL, whilst maintaining business continuity.	Must have
COR02	Core	The Supplier will simplify development (single responsibility for a service, well defined interfaces, improved automatable testing, reducing dependencies).	Must have
COR03	Core	The Supplier will support and improve adoption and integration processes.	Must have
COR04	Core	The Supplier will enable the adoption of more asynchronous exchange of data (less blocking).	Must have

OFFICIAL

NFR01	Non-Functional	The Supplier will ensure high availability of the service – 24/7 x 365 with zero-downtime. The service must be available to a minimum of 99.5% of the expected operational times.	Must have
NFR02	Non-Functional	The Supplier will ensure the system is able to process a high throughput in excess of 70 million events per annum.	Must have
NFR03	Non-Functional	The Supplier will ensure the system is tolerant of expected and unexpected failure of a data centre.	Must have
NFR04	Non-Functional	The Supplier will ensure the system is tolerant of expected and unexpected failure of physical / virtualised hardware, including networks.	Must have
NFR05	Non-Functional	The Supplier will ensure the system is tolerant to expected and unexpected failure of upstream services such as databases.	Must have
NFR06	Non-Functional	The service must be able to scale out and up/down automatically based on changes in metrics.	Must have
NFR07	Non-Functional	The service must be able to reject and/or queue requests to protect the overall service.	Must have
NFR08	Non-Functional	The service must be load, stress and soak tested in line with future growth projections to ensure that the services ability to handle increasing volume of events is assured.	Must have
SD01	Software Development	The Supplier will develop and enhance Authentication and Access Control, based on the existing security technologies and control.	Must have

OFFICIAL

SD02	Software Development	The Supplier will develop performance and scalability of the solution allowing to process expected volumes and support new client services.	Must have
PAT01	Patching	The Supplier shall be responsible for the ongoing patching of all Operating Systems deployed within the platform.	Must Have
PAT02	Patching	The Supplier shall be responsible for the ongoing server patching of: 1. All applications that are included in the Supplier's base template for a given operating system 2. Any underpinning database storage technology 3. All webserver / services.	Must Have
PAT03	Patching	The Supplier shall ensure all Anti- virus definitions are up to date.	Must Have
PAT04	Patching	The Supplier shall be responsible for monitoring Operating System and application security patch alerts for applications managed by the Supplier.	Must Have
PAT05	Patching	The Supplier shall notify the Authority when a critical security patch is released for an Operating System or Application managed by the Supplier within a time period agreed with the Authority.	Must Have
PAT06	Patching	The Supplier shall provide a patching policy document that will need to be approved for use, by the appropriate Home Office teams.	Must Have

OFFICIAL

PAT07	Patching	The Supplier shall implement a process to ensure new patches are not promoted to the FIL production environment without testing in a non-production environment first.	Must Have
NET01	Network Management	The Supplier shall be responsible for the configuration of all network devices in the platform via scripts that are maintained in a source control repository.	Must Have
DOC01	Documentation	The Supplier shall maintain, where appropriate, technical documentation, and ensure all documentation is current. This includes but is not limited to; High Level Designs Low Level Designs Schemas and Interface Control Documents User and onboarding guides Platform specific server specification and configuration Storage network configuration Backup and Disaster Recovery.	Must Have
DOC02	Documentation	The Supplier shall submit any changes to Supplier authored documentation to the Authority for review, and approval if required.	Must Have
SEC01	Security	The Supplier is responsible for complying with, and inputting to the Authority's security operating model, and will collaborate proactively with the Authority's security management teams as part of delivering new or existing services.	Must Have

OFFICIAL

SEC02	Security	The Supplier shall ensure continued development, implementation, and maintenance of a robust, scalable security solution in conjunction with the HO DDaT security architecture team.	Must Have
SEC03	Security	The Supplier, if appropriate, shall be responsible for installing Authority/Policing issued certificates to enable TLS on the platforms.	Must Have
SEC04	Security	The Supplier shall ensure that certificate renewals can be managed without impacting the service.	Must Have
SEC05	Security	The Supplier will align their delivery approach and practices with EBSA (Environment Build, Support and Administration) security standards.	Must Have
SEC06	Security	The Supplier shall ensure all team members have Security Clearance. Access to Home Office Systems will be granted following appropriate security checks and end user device agreement completed.	Must Have
BAC01	Backup	The Supplier shall retain each SQL backup until a newer backup is available.	Must Have

OFFICIAL

BAC02	Backup	The Supplier shall perform differential SQL transaction log hourly backups every hour.	Must Have
BAC03	Backup	The Supplier shall retain hourly SQL transaction logs for 24 hours.	Must Have
BAC04	Backup	The Supplier shall perform differential SQL Transaction log daily backups every 24 hours.	Must Have
BAC05	Backup	The Supplier shall retain differential SQL Transaction log daily backups for 11 days.	Must Have
USM01	User Management	The Supplier shall control access to the Admin user account. Only by authorisation by the Authority may a user be granted access to the Admin accounts.	Must Have
USM02	User Management	The Supplier shall revoke an individual's access to the Admin account on direction by the Authority.	Must Have

OFFICIAL

BC01	Business Continuity	Due to the criticality of the FIL it is crucial that the appropriate Business Continuity and Disaster Recovery mechanisms are implemented by the Supplier to mitigate the risk of any break in service continuity, including the duplication of key data hosting environments and related services, and to maintain the delivery of critical services.	Must Have
BC02	Business Continuity	<p>The Supplier will need to maintain a high-level awareness of cross-cutting business continuity and disaster recovery requirements across the programme.</p> <p>From time to time, MBTP will validate their BC/DR plans and the Supplier will provide support to the operational teams as required.</p>	Must Have
DR01	Disaster Recovery	The Supplier shall provide a Disaster Recovery capability to meet a Recovery Time Objective (RTO) of 4 hours.	Must Have
DR02	Disaster Recovery	The Supplier is required to implement a backup solution that enables a near zero Recovery Point Objective (RPO) to guard against data loss.	Must Have
DR03	Disaster Recovery	The Supplier shall host the Disaster Recovery capability for both Production and Quality Assurance Environments in a geographically different data centre to the respective primary sites for the environments.	Must Have

OFFICIAL

DR04	Disaster Recovery	The Supplier shall provide Disaster Recovery Designs (LLD and HLD) for the FIL.	Must Have
DR05	Disaster Recovery	The Suppliers DR solution will be available at point of Go-Live.	Must Have
LIC01	Licensing	The Supplier shall manage all licenses for all the installed software and operating systems on the FIL Platform whilst leveraging all Government discounts from the software vendors.	Must Have
APP01	Application	The Supplier shall provide a Software Catalogue that lists the set of software applications the Supplier supports (install, configuration, maintenance, and patching) in the environment.	Must Have
APP02	Application	The Supplier shall provide a mechanism for the Authority to add Software applications to the Supplier's Software Catalogue.	Must Have
TES01	Test Management	The Supplier will be responsible for testing up until autosit and not beyond this environment. The Supplier will support this testing and provide any automation which has been completed prior to that point. Automated testing is the default approach to testing in the Home Office, manual testing is by exception.	Must Have

OFFICIAL

TES02	Test Stages	The Supplier shall be accountable for the following Functional testing stages: Unit/Component integration testing (If applicable) Accessibility Testing (If Applicable) Infrastructure Build Testing System Testing Network connectivity Testing Data Migration Testing Regression Testing Infrastructure performance testing.	Must Have
TES03	Test Stages	The Supplier shall be accountable for the following Functional testing stages: Operational Acceptance Testing Performance testing (including peak, soak and stress) Security Testing Service Management Testing.	Must Have
TES04	Test Delivery	The Supplier shall support the customer assurance of all test deliverables and test execution in the form of quality reviews and test witnessing.	Must Have
TES05	Test Delivery	The Supplier shall provide the Authority with 10 days' notice of commencement of a Test Stage and provide all reasonable access to enable test execution and test witnessing.	Must Have
TES06	Test Delivery	The Supplier shall, on the date specified in the Test Plan perform the following: <ul style="list-style-type: none"> • Confirm resources, accommodation, equipment and facilities are in place to support testing. • Confirm customer access and roles are in place to support any witnessing or test execution activity including access to Supplier tooling for test and defect management. • Confirm all test specification and data are complete and ready for the Test Stage. 	Must Have

OFFICIAL

		<ul style="list-style-type: none"> Confirm the defect threshold has not been exceeded from other test stages and if so seek Authority approval to proceed based on proposed mitigations. Issue a draft test completion report for Authority approval. 	
TES07	Test Delivery	The Supplier shall maintain daily records of all test results.	Must Have
TES08	Test Delivery	The Supplier shall provide full support to connect all test environments, end-to-end to Customer provided official environments.	Must Have
TES09	Test Delivery	The Supplier shall provide Simulators and Stubs as needed to support Customer Test Stages.	Must Have
TES10	Test Delivery	The Supplier shall operate a Defect Management Process (DMP).	Must Have
TES11	Test Delivery	Defects raised during Testing shall be recorded in a suitable Defect Management Tool (DMT).	Must Have

OFFICIAL

TES12	Test Delivery	Defects raised during Testing shall be recorded by the Authorities Defect Management Tool (DMT).	Should Have
TES13	Defect classification	<p>The Supplier shall categorise defects using the following Defect Severity Level classifications:</p> <p>S1 - Critical - The failure causes system to crash, data loss or application failure such that it results in severe impact to one or more business processes, for which NO satisfactory workaround exists.</p> <p>S2 - High - The failure causes major impairment of one or more critical business functions, irrespective of whether a workaround exists; or the failure causes major impairment to one or more non-critical business functions for which a satisfactory workaround does NOT exist.</p> <p>S3 - Medium - The failure causes minor impairment of one or more critical or non-critical business functions, irrespective of whether a workaround exists; or the failure causes a major impairment to one or more non-critical business functions for which a satisfactory workaround does exist.</p> <p>S4 - Low - The failure is a cosmetic inconvenience / annoyance such that it does NOT hinder a user's ability to carry out business functions OR decrease their productivity.</p>	Must Have
TES14	Defect Thresholds	<p>The Supplier shall ensure that the defect thresholds proposed for each test stage shall be no greater than:</p> <p>Zero S1 defects Zero S2 defects; and</p> <p>Any unresolved S3 - S4 defects have agreed resolution actions, planned closure dates and do not represent an unacceptable risk to the solution under test.</p>	Must Have

OFFICIAL

TES15	Defect Thresholds	The Authority shall confirm the classification of any defect unresolved at the end of a test stage in consultation with the Supplier.	Must Have
SM01	Service Management	The Supplier will support the Authority's service management functions in order to meet performance, cost and functional service obligations delivered by the 2nd line support teams, including event monitoring, both in terms of security monitoring and common support alerting.	Must Have
SM02	Service Management	The service operates 24/7 x 365. The Supplier will ensure the service availability is at 99.5% excluding events triggered by other services, scheduled maintenance and shutdowns in response to incidents such as DOS attacks.	Must Have
SM03	Service Management	The Supplier will ensure that its service support includes integration points with the Authority's Service capabilities and processes, including, but not limited to: Service Desk; Incident Management; Problem Management; Change Management; Release and Deployment Management; Major Incident Management; Knowledge Management; Software Asset and Configuration Management.	Must Have
SM04	Service Management	The Supplier will include the following service delivery processes: Service Level Management; IT Financial Management; Capacity Management; Availability and Performance Management; IT Service Continuity Management; Security Management; Continuous Service Improvement; Service Reporting; Service Transition.	Must Have

OFFICIAL

SM05	Service Management	The Supplier will provide their services as a Level 3 support capability in accordance with HO DDaT's MBTP incident management processes where applicants or caseworkers can report issues. These issues are triaged and resolved by Level 2 Support Teams, if they are able to, based on Work Instructions for known errors.	Must Have
SM06	Service Management	If Level 2 are unable to resolve an incident because it would require a change in the source code or a change in the way the product functions, data errors, or is overall too technically complex; the incident will be raised to the L3 team (Supplier's support team) to conduct a Root Cause Analysis. The L3 team are responsible for: <ul style="list-style-type: none"> 1. Root Cause Analysis 2. Code Change 3. Design Changes 4. Data Corrections 5. Work Instructions 	Must Have
SM07	Service Management	Reporting Incident - As part of their Level 3 support and development activities or in their regular monitoring of the system, the Supplier is responsible for raising any issues they see in Production with the L2 Support teams so appropriate triage and Incident Management processes can start.	Must Have
SM08	Service Management	The Supplier will be assigned incidents for investigation within Level 3 support activities and as investigation progresses, the Supplier will provide updates within the Authority's Toolset.	Must Have
SM09	Service Management	Within the scope of the working hours agreed for the Supplier service, the Supplier will support Level 2 teams in order to meet the stated Incident Resolution Times and their agreed service level agreements. All incident start times are measured from the moment the incident record is registered in the Authority's Toolset.	Must Have

OFFICIAL

SM10	Service Management	The Supplier will ensure that they Investigate and resolve incidents in line with the following criteria:		Must Have
		Priority	Description	
		Resolution Target	Response Target	
		P1	Service is unavailable for all consumers	
		100% < 4 Hours	< 1 Hour	
P2	Part of the service is unavailable e.g. Like for Like document update	100% < 8 Hours	< 1 Hour	
P3	Part of the service is unavailable, but a workaround is available to cover the interim period whilst the issue is handled.	95% < 3 Days	< 8 Hours	
P4	Little to no impact to existing service, usually cosmetic issues. General requests of queries relating to the service.	95% < 5 Days	< 24 Hours	
SM11	Service Management	<p>Service Support Hours</p> <p>Priority 1 Service Outages: On Call Coverage Every day: 24 x 365 (includes all national holidays)</p> <p>All Other Priorities: 09.00 – 17.30 UK Time, Monday to Friday working days (classed as 1 day for resolution targets).</p>		Must Have

OFFICIAL

SM12	Service Level Management and Service Reporting	<p>The Supplier is responsible for inputting into the Authority's Service Level Management processes by managing and reporting service performance to the Authority on a monthly basis, in a format to be mutually agreed between the Supplier and the Authority.</p> <p>This includes metrics relating to the availability of the services, and adherence to Service Levels relating to the Supplier's performance. The Authority may also request that other performance indicators are included in reporting if they are determined as important metrics that underpin effective running of the services.</p>	Must Have
PROB01	Problem Management	The Supplier is required to deliver a collaborative capability providing both proactive and reactive problem management support under the governance of the Authority's Service Desk Problem Management. This will be in accordance with Authority's Problem Management operating model.	Must Have
PROB02	Problem Management	As part of their Level 3 support activities, the Supplier will investigate and provide root cause analysis reports on problems assigned to them. It is expected that from time to time the Supplier will also collaborate with other delivery teams as part of analysing complex problems.	Must Have
OPS01	Operations Management	In the day to day systems management and operational support of the service, the Supplier shall work in a Level 3 support capacity in line with requirements assigned to them by the relevant Level 2 teams. The Supplier will be responsible for ensuring an effective capacity for supporting the live service in production.	Must Have

OFFICIAL

OPS02	Operations Management	As part of operations management, the Supplier will be responsible for delivering, maintaining, and improving operational features (such as alerting and monitoring) that support the Authority's teams in monitoring the daily health of the services.	Must Have
CHGR01	Change and Release Management	The Supplier will deliver all changes into the Live Services in accordance with the Authority's Change Management operating model. There is a responsibility for delivery teams to understand if releases are Impacting or Non-Impacting. The Supplier is also responsible for understanding if a release will impact other Authority services, and in accordance with the Authority's Change Management operating model will take steps to ensure that other delivery teams are aware of the release in good time for them to take measures to protect their services.	Must Have
CHGR02	Change and Release Management	For all releases, the Supplier will follow the Authority's existing Change Management process. Any potential releases will need to have a release note along with the results of testing. These release artefacts will need to be assessed and approved by the Core Delivery Lead, Quality Assurance Lead and a member of the Change & Release Management Team. The approval process is managed in the Authority's Slack instance which the Supplier will be given access to.	Must Have
DEP01	Release and Deployment	Release Assurance and Integration activities deliver enhancements, maintenance and new services to the enterprise, but they can also present risk to the controlled environments and services of the Authority's Live Services estate. The Supplier will be required to work with the Authority's Change & Release Management Team in order for that team to raise all the required release and deployment approvals.	Must Have

OFFICIAL

DEP02	Release and Deployment	The Supplier will provide deployment support to operational teams. This may be outside of the core hours by agreed exception.	Must Have
DEP03	Release and Deployment	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 delivery approach through agreed pipeline release cycles. In order to minimise error, the Supplier should endeavour to automate deployments within their schedules.	Must Have
TRA01	Transition	The Supplier will deliver all features, significant releases, and new services in accordance with the Authority's Service Transition operating model.	Must Have
TRA02	Transition	<p>The Supplier will proactively engage with the Authority's service transition team, and will take a collaborative approach to completing the Service Acceptance and Assurance actions deemed necessary by the Authority's Service Transition team to ensure that the Authority's support team is in a position to manage the delivered service effectively.</p> <p>Typically, the level of assurance required depends on the impact and complexity of the delivery, and the Supplier and the Authority's Service Transition team will work collaboratively to determine the right approach on a case by case basis.</p>	Must Have
KT01	Knowledge Transfer	The Supplier will be required to ensure knowledge transfer to Home Office civil servant staff who are embedded within the Supplier's teams. This will be an ongoing process, and not confined to the Contract exit provisions.	Must Have

OFFICIAL

LWA01	Location and Working Arrangements	The MBTP Programme is based in Croydon. The Supplier resources working at these locations will need to ensure they comply with guidance provided by the Portfolio Security Team.	Must Have
LWA02	Location and Working Arrangements	There is no estate allocation for the Supplier and they are expected to work from home or from their own business premises. Supplier's staff will still be able to attend site and utilise drop in seats with prior agreement.	Must Have

7. KEY MILESTONES AND DELIVERABLES

- 7.1 Find below a list of our near-term key milestones and deliverables that are critical to the fulfilment of the Contract. Note that over the course of time additional milestones and deliverables will be mutually agreed once the detail is known.


The roadmap for beyond 2022 is currently being defined and it is anticipated that the Supplier will also deliver the roadmap once finalised.

Work in the FIL Product roadmap includes work from multiple programmes, and work to implement the strategic architecture, as well as continuous improvement, technical debt and accessibility improvements.

- 7.2 The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	Continuous improvements on existing integrations	Ongoing
2	Transition of components to BESS MSK infrastructure	██████████
3	Publish components migrated to Generic Publisher	██████████
4	AUK Convergence	██████████
5	Sponsorship Integration	██████████

OFFICIAL

6	Transition of components to other services	
7	Decommissioning of FBIS Integration Layer Service	Within the lifetime of the FBIS programme

8. MANAGEMENT INFORMATION/REPORTING

- 8.1 The Supplier is required to manage the effective delivery of the work using agile management methods (including running agile ceremonies, measuring performance, configuring and using Jira and Confluence to this end) and project support functions. This includes and is not limited to;
- 8.1.1 Daily Stand-ups
 - 8.1.2 Managing dependencies with other delivery workstreams and participating in planning sessions
 - 8.1.3 Providing metrics/visibility of the work
 - 8.1.4 Weekly backlog refinement sessions (or more/less frequently if required)
 - 8.1.5 Weekly backlog estimation sessions (or more/less frequently if required)
 - 8.1.6 Fortnightly product demonstrations as appropriate
 - 8.1.7 Fortnightly sprint retrospectives
 - 8.1.8 Fortnightly sprint planning sessions
 - 8.1.9 Reporting to Delivery Board
 - 8.1.10 The Supplier will be required to ensure knowledge transfer to Home Office civil servant staff who may join the team to work alongside the Supplier. This will be an ongoing process, and not confined to the Contract exit provisions.
- 8.2 The Authority requests that the Supplier submits management information in the form of monthly Balanced Scorecard status reports and present at a monthly face to- face meeting.
- 8.3 The Balanced Scorecard process is detailed in Attachment 3b. Further guidance on the process will be provided as and when required. The Balanced Scorecard approach helps drive consistency of performance measurement

OFFICIAL

across the supplier base. The Authority and the Supplier take a collaborative approach; Authority's assessors across the FIL Programme who interface with the Supplier give feedback in a prescribed template to the Commercial team. The Supplier must also self-certify its performance against the scorecard and also provide this to the Commercial Team in a monthly Balanced Scorecard report.

- 8.4 The established Scorecard KPI's will measure Supplier's performance on a monthly basis. The Authority will provide feedback against service levels and KPI's to the Supplier each month.
- 8.5 The monthly acceptance process will also capture performance to milestone targets and agreed plans; the Authority's project manager will include an assessment of Supplier performance when approving supplier acceptance certificates.
- 8.6 The Balanced Scorecard status report template to be used by the Supplier is provided in Attachment 3b. Such reports should include, as a minimum:
 - 8.6.1 Delivery performance against SOW
 - 8.6.2 Spend to date against SOW
 - 8.6.3 Identification of customer dependencies
 - 8.6.4 Highlighting any potential delivery issues
 - 8.6.5 Self-certification of performance against the Balanced Scorecard Quadrants (P2P Process, Service Requests & Resourcing, Partnering, Value Add & Delivery)

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

10. CONTINUOUS IMPROVEMENT

- 10.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration, in accordance with Section 17 of the RM6100 Framework Terms and Conditions.

OFFICIAL

- 10.2 The Supplier should aim to utilise monthly Balanced Scorecard review meetings to present new ways of working to the Authority, and such new ways of working should be presented no less frequently than once every quarter.
- 10.3 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.
- 10.4 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
- 10.5 The Supplier should present new ways of working to the Authority during monthly Contract review meetings.
- 10.6 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.
- 10.7 The Supplier is expected to monitor FIL performance and make necessary changes to meet & exceed Portfolio Non-Functional Requirements (NFRs) and provide CLI-level availability.
- 10.8 The Supplier is expected to monitor FIL and ensure it can scale in line with projected user volumes driven by future projects and initiatives.
- 10.9 The Supplier is expected to identify and address platform resilience concerns.
- 10.10 The Supplier is expected to review FIL monitoring and reporting capability – deliver improvements in monitoring to pre-empt and issue and improved logging to reduce time for support team to complete investigation.
- 10.11 The Supplier is expected to deliver new functional changes requested by the business that require changes to core capability.
- 10.12 The Supplier is expected to meet the definition of done including aligning with the HO DDaT test strategy.
- 10.13 The Supplier is expected to provide and manage a fully automated CI pipeline for deploying and managing the FIL, utilising CI technologies (such as Jenkins, Docker and Kubernetes)
- 10.14 The Supplier shall lead on innovation engineering in the agile delivery lifecycle.
- 10.15 The Supplier is expected to lead on performance engineering and being accountable for the performance of the FIL.
- 10.16 The Supplier shall ensure continued development, implementation and maintenance of a robust, scalable security solution in conjunction with the HO DDaT security architecture team.

OFFICIAL

- 10.17 The Supplier is expected to provide a Dev Ops capability - Release pipeline improvements/optimisation initiatives/ maintenance of Jenkins environments.
- 10.18 The Supplier is expected to support and maintain performance and availability of the FIL. In the event of Live Service incidents, they are expected to collaborate with Live Service teams to resume services, following standard Live Service processes where required.

11. SUSTAINABILITY

- 11.1 The Supplier must ensure they are committed to, and acting to support the UK Governments strategy to achieving Net Zero emissions by 2050. This includes but is not limited to;
- 11.1.1 Reducing carbon footprint
 - 11.1.2 Improving resource use and efficiency
 - 11.1.3 Using sustainable products and processes

12. QUALITY

- 12.1 Required quality and standard accreditations that the Supplier should hold:
- 12.1.1 ISO9001
- 12.2 The Potential Provider will have awareness of:
- 12.2.1 Cyber Essentials
 - 12.2.2 Home Office Digital Strategy - <https://www.gov.uk/government/publications/home-office-digital-data-and-technology-strategy-2024/home-office-digital-data-and-technology-strategy-2024>
 - 12.2.3 Government Service Design Manual - <https://www.gov.uk/service-manual>
 - 12.2.4 HMG Security Policy Framework - <https://www.gov.uk/government/publications/security-policy-framework>
 - 12.2.5 Government Security Classification Policy - <https://www.gov.uk/government/publications/government-security-classifications>
 - 12.2.6 GDS Service Manual standards and Policies - <https://www.ncsc.gov.uk/>

OFFICIAL

13. PRICE

- 13.1 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.
- 13.2 Pricing should be submitted on a capped time and materials basis for development and in-hour support and fixed price for the out of hours (including any call out charges) monthly retainer.
- 13.3 Pricing should assume that this arrangement falls within a consideration of IR35, and therefore all and any resources deployed to deliver the services must be subject to Tax and NIC being deducted at source and reported/paid to HMRC via their Real Time information system. That is, resources deployed should either be employees of the supplier or any supply chain partners or operate through FCSA accredited Umbrella Company's or PAYE providers.
- 13.4 In the event that the Supplier needs to contract with Subject Matter Experts on an outcome's basis for delivery of aspects of the contract during the term of the contract then this can be discussed with the Authority. Such work would then be contracted within an individual SOW specifically for the work to be performed.
- 13.5 Under the new contract, FIL will be managed through SOWs for deliverables that are agreed in advance with the supplier these could vary in duration over the course of the contract but for the purposes of evaluation the example SOW covers a six-month period. Potential Providers are asked to price against a baseline six-month exemplar SOW reflecting the service and structure (organisation) today, its management and its level of support, tickets, events, and any ongoing CI known today as a representative example of the level of effort required over a rolling six-month delivery period. This SOW is provided in Attachment 4b. Please price using the baseline six-month exemplar SOW. To obtain the total contract cost there will be an assumption of the same level of effort for future periods, essentially carrying the first six-month price over the 3-year period. The actual level of effort required will be determined by operational need and the prevailing Authority/Supplier resource level mix at the future time so the size of future SOWs may be larger or smaller than that considered for baseline today.
- 13.6 There may also be discrete SOWs for continuous improvement (CI) and new capabilities agreed over the term. As the scope of CI and new capabilities over the next three years is not yet fully understood at this time, such SOWs could be priced on a fixed, capped time and materials or a time and materials basis in the future. The pricing build-up for such new SOWs during the contract shall

OFFICIAL

use the charging rates provided in the Attachment 4 Excel template 'as bid' by the Potential Provider.

- 13.7 Supplier day rates as recorded on the Rate Card tab of the Price Model Template will be fixed for the three-year term and the appointed Supplier will be asked to be compliant with the Maximum rates in the Optimus Target Rate Card. The Tender caps the maximum daily rate payable to any SFIA grade in accordance with the Target Rate Card. Any bid proposing a daily rate in excess of this will be considered non-compliant.
- 13.8 We will investigate any bid we consider to be abnormally low.
- 13.9 All prices must be for the duration of the Call-Off Contract and priced in sterling. Please note that Government policy places the burden of exchange rate fluctuations on the Supplier, who shall be expected to absorb the impact of these within and across their contracts.

14. STAFF AND CUSTOMER SERVICE

- 14.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
- 14.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard, and such staff shall not have dissimilar qualifications or experience to those highlighted within the supplier bid.
- 14.3 The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

15. SERVICE LEVELS AND PERFORMANCE

- 15.1 The Authority will measure the quality of the Supplier's delivery by measurement of delivery service against the required service levels and KPIs that are set out in the table below. The Supplier's performance will be assessed against such service levels and KPIs.

- 15.2 Proposed KPIs and Service Levels:

KPI	Metric	What information is required to measure this KPI?	How will the KPI be measured?	Red	Amber	Green
Delivery	As agreed between the Supplier and the	Capability requirements and costs to be agreed	Cost/time/quality	Specific to each requirement	Specific to each requirement	Specific to each requirement

OFFICIAL

Attachment 3 – Statement of Requirements

Leah Emery

© Crown copyright 2018

V1.7 29th March 2022

	Authority on a requirement-specific basis within each SOW.	within agile approach				
Quality	Deliverables of acceptable quality	Deliverable provided to the Authority. Provision of acceptance certificates	Acceptance certificates awarded without rework of deliverable	Specific to each requirement	Specific to each requirement	Specific to each requirement
Cost	Partner to work to costs or less unless otherwise agreed	Spend to-date, provided to the Authority by Supplier.	Monthly invoicing. Bi-weekly checkpoint meetings, Balanced Scorecard report (costs to-date)	Above agreed budget	At budget	Less than budget
Continuous improvement	Partner to work with FIL team to identify and deliver incremental improvements to ways of working and the product	Qualitative/NA	Biweekly checkpoint meetings. Balanced Scorecard meetings. Improvements to be identified on an ad-hoc basis	No delivery of innovation or improvement during previous quarter	Delivery of one innovation or improvement per quarter	Delivery of two or more innovations or improvements per quarter
Contract Management	Balanced Scorecard	Supplier to meet Balanced Scorecard measures	Per Balanced Scorecard Process, as detailed within Attachment 3b	One quadrant or more rated Red	One quadrant or more rated Amber	All quadrants rated as Green
Contract Management	Balanced Scorecard	Supplier to attend monthly Balanced Scorecard Meetings	Attendance at meetings	Two or more meetings missed during the previous 12 months.	One meeting missed during the previous 12 months.	Attendance at all meetings during the contract term.
Social Value	Covid-19 Recovery	Help communities to manage and recover from the impact of Covid-19	Monthly updates as part of the Balanced Scorecard Process Annual report to document continued	Specific to supplier bid	Specific to supplier bid	Specific to supplier bid

OFFICIAL

			demonstration of how you are helping communities manage and recover from the impact of Covid-19			
Social Value	Equal Opportunity	Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce	Monthly updates as part of the Balanced Scorecard Process Annual report to demonstrate what action has been taken to tackle inequality in employment, skills and pay in the contract workforce	Specific to supplier bid	Specific to supplier bid	Specific to supplier bid.

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

- 16.1 All Supplier staff working on FIL must hold SC prior to being able to commence working.
- 16.2 Direct access to the solution must be undertaken by UK based resources that can pass the HMG vetting process to SC.
- 16.3 The Supplier must pass the Home Office supply chain management process.
- 16.4 The Supplier must pass on any security requirements from the Authority to any Sub Contractors.
- 16.5 The Supplier must ensure any Sub Contractors can pass the Home Office supply chain management process.
- 16.6 The Supplier and Sub Contractors must not be from a state deemed hostile or high threat to the UK.
- 16.7 The Supplier or Sub Contractors must not be under any direct control of any foreign Government and be an independent autonomous entity.

OFFICIAL

17. PAYMENT AND INVOICING

- 17.1 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
- 17.2 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs. All invoices and supporting information must include the purchase order reference number and contract reference number.
- 17.3 Invoices should be submitted via email to [REDACTED] or by post to: [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
- 17.4 For any queries regarding invoicing and payment, please contact the shared Service Centre by emailing [REDACTED]
[REDACTED]

18. CONTRACT MANAGEMENT

- 18.1 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. Please refer to Section 8 of this document for more details of the Balanced Scorecard process.
- 18.2 Attendance at meetings shall be at the Supplier's own expense.
- 18.3 On the basis of the information available, the Home Office does not consider that TUPE will apply to this procurement. However, Tenderers will need to make their own assessment of whether, and if so, to what extent, TUPE will apply. Tenderers should obtain their own legal advice on the application of TUPE. It remains the Tenderer's responsibility to ensure that the Tender takes full account of all the relevant circumstances. The Tenderers will also have no reliance on the information provided by the Home Office and the Home Office gives no warranty, guarantee or assurance as to the accuracy of the information provided, and is not responsible for errors or omissions in it.

19. LOCATION

- 19.1 The location of the Services will be carried out at the Suppliers own site, or as agreed, the Home Offices Croydon hub.
- 19.2 There is no estate allocation for the Supplier and it is expected to work from home or from their own business premises. Supplier staff will still be able to attend site and utilise drop in seats with prior agreement.

OFFICIAL

