Technology Services 2 Agreement RM3804
Framework Schedule 4 - Annex 1

Order Form

In this Order Form, capitalised expressions shall have the meanings set out in Call Off Schedule 1 (Definitions), Framework Schedule 1 or the relevant Call Off Schedule in which that capitalised expression appears.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of the Call Off Contract for the duration of the Call Off Period.

This Order Form should be used by Customers ordering Services under the Technology Services 2 Framework Agreement ref. RM3804 in accordance with the provisions of Framework Schedule 5.

The Call Off Terms, referred to throughout this document, are available from the Crown Commercial Service website http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3804

The Customer must provide a draft Order Form as part of the Further Competition Procedure.

Section A
General information

This Order Form is issued in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

Customer details
Customer organisation name Food Standards Agency
Billing address Your organisation's billing address - please ensure you include a postcode Foss House, Kingspool, Peasholme Green, York, YO1 7PR
Customer representative name The name of your point of contact for this Order ███████
Customer representative contact details Email and telephone contact details for the Customer's representative ████████████████

Supplier details

Supplier name
The Supplier organisation name, as it appears in the Framework Agreement
Little Fish (UK) Ltd

Supplier address
Supplier's registered address
Price House, 37 Stoney Street, Nottingham, NG1 1LS

Supplier representative name
The name of the Supplier point of contact for this Order
▮▮▮▮▮▮▮▮

Supplier representative contact details
Email and telephone contact details of the supplier's representative
▮▮▮▮▮▮▮▮▮▮▮▮

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

Click here to enter text.

Section B
Overview of the requirement

Framework Lot under which this Order is being placed _Tick one box below as applicable (unless a cross-Lot Further Competition)_		**Customer project reference** _Please provide the customer project reference number._
1. TECHNOLOGY STRATEGY & SERVICES DESIGN	☐	FS430637
2. TRANSITION & TRANSFORMATION	☐	**Call Off Commencement Date**
3. OPERATIONAL SERVICES		_The date on which the Call Off Contract is formed – this should be the date of the last signature on Section E of this Order Form_
a: End User Services	☒	
b: Operational Management	☐	
c: Technical Management	☐	01/09/2021
d: Application and Data Management	☐	
4. PROGRAMMES & LARGE PROJECTS		
a. OFFICIAL	☐	
a. SECRET (& above)	☐	

Call Off Contract Period (Term)

A period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Initial Term – Months (Years)	Extension Options – Months (Years)	Maximum permissible overall duration – Years (composition)
1	24 (2)	-	2
2	36 (3)	-	3
3	60 (5)	-	5
4	60 (5) *	12 + 12 = 24 (1 + 1 = 2)	7 (5+1+1) *

* *There is a minimum 5 year term for this Lot*

Call Off Initial Period Months

36

Call Off Extension Period (Optional) Months

12 + 12 (2 separate 12-month extension periods)

Minimum Notice Period for exercise of Termination Without Cause   90

(Calendar days) *Insert right (see Call Off Clause 30.7)*

Additional specific standards or compliance requirements

Include any conformance or compliance requirements over and above the Standards (including those listed at paragraph 2.3 of Framework Schedule 2) which the Services must meet.
List below if applicable

NA

Customer's ICT and Security Policy

Where the Supplier is required to comply with the Customer's ICT Policy and Security Policy then append to this Order Form as a clearly marked document

FS430637_006 FSA Acceptance Into Service Procedure
FS430637_007 FSA Change Management Procedure
FS430637_008 FSA Incident Management Procedure
FS430637_009 FSA Security Incident Procedure 2019
FS430637_010 FSA Problem Management Process
FS430637_011 FSA Knowledge Management Procedure
FS430637_012 FSA Service Asset & Configuration Mgt Procedures
FS430637_013 FSA Supplier Access Policy August 2019 v1
FS430637_014 FSA IT Acceptable Use Policy Nov 2020 v3.2
FS430637_016 FSA Request Fulfilment
FS430637_018 FSA Patching Policy Sept 2019 1.1

FS430637_006 FSA Acceptance Into Servi	FS430637_007 FSA Change Management	FS430637_008 FSA Incident Management	FS430637_009 FSA Security Incident Proc	FS430637_010 FSA Problem Managemen	FS430637_011 FSA Knowledge Managem

FS430637_012 FSA Service Asset & Confi	FS430637_013 FSA Supplier Access Policy	FS430637_014 FSA IT Acceptable Use Policy	FS430637_016 FSA Request Fulfilment.do	FS430637_018 FSA Patching Policy Sept 2

Security Management Plan

The Supplier will create an information Security Management Document Set to document how they will comply with the specific FSA security requirements to be approved by the Head of Security at the FSA. This will be completed as part of On-Boarding the supplier before the service begins.

3

Section C
Customer Core Services Requirements

Please provide details of all Services required including the locations where the Supplier is required to provide the Services Ordered.

Services
List below or append as a clearly marked document to confirm the Services which the Supplier shall provide to the Customer (which could include the Customer's requirement and the Supplier's response to the Further Competition Procedure). If a Direct Award, please append the Supplier's Catalogue Service Offer.

Please see Annex A for the Specification of Requirements and the Suppliers responses to the ITT. This make up the services to be carried out under this contract.

On occasion the FSA may require the supplier to engage on project work as part of this service, but not covered by the monthly service charge. This shall be commissioned using the work package template found under Annex B.

Location/Site(s) for provision of the Services
This service will be delivered remotely by the Supplier, with the occasional requirement to visit FSA Offices/Sites.

Additional Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM3804 CCS webpage. The document is titled RM3804 Alternative and additional t&c's v4.
Those Additional Clauses selected below shall be incorporated into this Call Off Contract

Applicable Call Off Contract Terms	Optional Clauses
Additional Clauses and Schedules	*Can be selected to apply to any Order*
Tick any applicable boxes below	*Tick any applicable boxes below*
A: SERVICES – Mandatory **The following clauses will automatically apply where Lot 3 services are provided (this includes Lot 4a & 4b where Lot 3 services are included).** ☒	C: Call Off Guarantee ☐
	D: Relevant Convictions ☒
A3: Staff Transfer	E: Security Requirements ☒
A4: Exit Management	
A: PROJECTS - Optional	F: Collaboration Agreement Where required please complete and append to this Order Form as a clearly marked document (see Call Off Schedule F) ☐
A1: Testing ☐	

A2: Key Personnel	☒	G: Security Measures	☐

B: SERVICES - Optional
Only applies to Lots 3 and 4a and 4b

		H: MOD Additional Clauses	☐
B1: Business Continuity and Disaster Recovery	☒		
B2: Continuous Improvement & Benchmarking	☒	**Alternative Clauses**	
B3: Supplier Equipment	☐	*To replace default English & Welsh Law, Crown Body and FOIA subject base Call Off Clauses*	
B4: Maintenance of the ICT Environment	☐	*Tick any applicable boxes below*	
B5: Supplier Request for Increase of the Call Off Contract Charges	☐	Scots Law Or	☐
B6: Indexation	☐	Northern Ireland Law	☐
B7: Additional Performance Monitoring Requirements	☐	Non-Crown Bodies	☐
		Non-FOIA Public Bodies	☐

Collaboration Agreement *(see Call Off Schedule F) This Schedule can be found on the RM3804 CCS webpage. The document is titled RM3804 Collaboration agreement call off schedule F v1.*

Not Applicable

Licensed Software Where Software owned by a party other than the Customer is used in the delivery of the Services list product details under each relevant heading below

Supplier Software

Click here to enter text.

Third Party Software

Click here to enter text.

Customer Property *(see Call Off Clause 21)*
Items licensed by the Customer to the Supplier (including any Customer Software, Customer Assets, Customer System, Customer Background IPR and Customer Data)
List below if applicable
ServiceNow Licenses.
Any Devices Shared with the supplier to enable them to carry out aspects of the contract.

Call Off Contract Charges and Payment Profile *(see Call Off Schedule 2)*

Crown
Commercial
Service

Contract Year	Y1	Y2	Y3	Y4	Y5
Fixed Monthly Charge	████	████	████	████	████
Fixed Annual Charge	████	████	████	████	████

Undisputed Sums Limit (£)
Insert right (see Call Off Clause 31.1.1)   ████████

Delay Period Limit (calendar days)
Insert right (see Call Off Clause 5.4.1(b)(ii))   NA.

Estimated Year 1 Call Off Contract Charges (£)
For Call Off Contract Periods of over 12 Months   ████████

Enhanced Insurance Cover
Where a specific Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Schedule 14 please specify below

No Enhanced Insurance cover required.

Transparency Reports *(see Call Off Schedule 6)*
If required by the Customer populate the table below to describe the detail (titles are suggested examples)

To be agreed between the FSA and Little Fish (UK) Ltd during the on-boarding of the service.

Quality Plans *(see Call Off Clause 7.2)*

Time frame for delivery of draft Quality Plans from the Supplier to the Customer – from the Call Off Commencement Date (Working Days)
Where applicable insert right   To be agreed between the FSA and Little Fish during On-boarding of the service.

Implementation Plan *(see Call Off Clause 5.1.1)*

RM3804 Order Form v4 - August 2019

Time frame for delivery of a draft Implementation Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) *Where applicable insert right. If a Direct Award, please append the Implementation Plan attached to the Supplier's Catalogue Service Offer.*	To be agreed between the FSA and Little Fish during On-boarding of the service.

BCDR *(see Call Off Schedule B1)*
This can be found on the CCS RM3804 webpage. The document is titled RM3804 Alternative and additional t&c's v4.

Time frame for delivery of a BCDR Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) *Where applicable insert right*	45 days

Disaster Period (calendar days)
Services with availability SLAs for 24/7/365 = 1 working day
All other services = 2 working days.

GDPR (see Call Off Clause 23.6)
Where a specific Call Off Contract requires the inclusion of GDPR data processing provisions, please complete and append Call Off Schedule 7 to this order form. This Schedule can be found in the Call Off Contract on the RM3804 CCS webpage

---

Supplier Equipment *(see Call Off Clause B3)*
This can be found on the RM3804 CCS webpage. The document is titled RM3804 Alternative and additional t&c's v4.
NA

Key Personnel & Customer Responsibilities *(see Call Off Clause A2)*
List below or append as a clearly marked document to include Key Roles

Key Personnel	**Customer Responsibilities**
List below or append as a clearly marked document to include Key Roles	*List below or append as a clearly marked document*
Customer Services Director Service Account Manager Service Delivery Manager Incident Manager Request Manager Major Incident Manager Service Desk Analysts	

Relevant Conviction(s)
Where applicable the Customer to include details of Conviction(s) it considers relevant to the nature of the Services.
List below or append as a clearly marked document (see Call Off Clause D where used)
As detailed in the Personnel Security requirements included in the Qualification and Service responses in Annex A.

RM3804 Order Form v4 - August 2019

Appointment as Agent *(see Call Off Clause 19.5.4)*
Insert details below or append as a clearly marked document

NA

SERVICE LEVELS AND SERVICE CREDITS *(see Part A of Call Off Schedule 3)*

Introduction

Suppliers will be required to provide the Incident Management element of this agreement using the following parameters:

- Core or 'working' hours 7:00am to 8:00pm Monday to Friday

- Non-core 8:00pm to 7:00am Monday to Friday plus weekends and bank holidays

There will be no Service Credit/Debit regime associated with this call-off. Instead the target achievement levels detailed in Table A will attract failure points where resolution targets are not met. Performance against SLAs must be monitored and reported on by the Supplier. The Supplier must also identify why they have not been achieved and what plans are being instigated to ensure that this does not continue.

Contact Management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved

Measure	Description	Target to be achieved in month
Call response	Telephone calls are answered within 20 seconds	90% of total calls
Email response	Emails are answered within 1 hour	90% of total emails
Chat response	Electronic chat to be responded to within 2 minutes	90% of total chat requests

Incident Management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved (i.e. attend Post Incident Reviews, provide Root Cause, Resolution, Avoidance and Remediation….):

RM3804 Order Form v4 - August 2019

Standard Incident Management Responsibilities for all suppliers include:

- Raising and maintaining incidents

- Triaging and prioritising incidents

- Providing regular and comprehensive updates

- Ensuring 3rd parties are provided with necessary information to enable resolution of incidents

The Supplier will carry out all Incident Management duties in accordance with the FSA's documented Incident Management procedures.

In the event of a P1 or P2 Incident major incident processes will be invoked, Supplier shall conduct a formal Problem Management review, which shall include undertaking a root cause analysis ("RCA") to determine the underlying cause of the Incident and providing guidance to support any activity required to amend the underlying cause.

Allocation of Incident levels (P1 – P4) will be done using the following table:

Table A – Incident Severity

Severity	Description	Response Time	Resolution Time*	Target to be achieved in month
P1	Severe business disruption: business unit or sub-unit unable to operate, critical components failed. Failure to meet technological minimums.	15 minutes from assignment of issue	4 hours	No more than 1 failure
P2**	Major business disruption: critical user(s) or user group unable to operate, or business unit experiencing significant reduction in system performance.	30 minutes from assignment of issue	8 hours for critical services, 8 working hours for non-critical services	No more than 1 failure
P3	Minor business disruption: single user unable to operate with no circumvention available	0.5 working day from assignment of issue	3 working days	Either 90% or above OR no more

P4	Minor disruption: single user or user group experiencing problems, but with circumvention available	1 working day from assignment of issue	3 working days	than 2 failures

* The Resolution Time starts when the incident is raised in Service Now and ends when the Incident is Resolved

** P2 major incident SLA will include security-related incidents (spam / phishing emails affecting 10 or more users) which are subject to a different process to major incident

Adherence to incident management responsibilities will also be assessed via reviews of completed incidents.

Service Desk Service Levels:

Measure	Description	Target to be achieved in month
First-time fix	Incidents submitted via phone or instant chat are resolved on a first-time fix basis where resolution responsibility resides with the service desk	70% of eligible incidents
P1 and 2 escalation notification	Major Incident escalation notification must occur, when required, within 15 minutes of a P1/2 incident being registered	No more than 1 failure
Re-assignment time	P3 and 4 incidents are re-assigned to the appropriate resolver group where resolution responsibility does not reside with the service desk within 1 working day	90% of eligible incidents
Breached tickets	Customer receives an update within 1 working day where a resolution SLA has been breached	90% of total incidents
Incident updates	Customer receives an update to at least the resolution times per incident type for in-progress incidents (e.g. update every 3 working days for in-progress P3 incident)	90% of eligible incidents
Incident quality checks	A minimum standard for incident ticket information to be agreed and a quality checking method to be determined	TBC

Request Management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved

Standard Request Management Responsibilities for all suppliers include:

- Carrying out request tasks within the allocated timescales

- Providing regular and comprehensive updates

The Supplier will carry out all Request Management duties in accordance with the FSA's documented Request Management procedures.

Description	Resolution Time	Target to be achieved in month
Access requests, including access to or creation of a distribution list, access to shared file / folder, shared mailbox, another person's email account	3 working days	90%
External sharing requests (e.g. working with teams, sharing with onedrive)	3 working days	90%
Restore an email / file	3 working days	90%
Password reset	1 hour	100%
Request for information	3 working days	100%
Breached tickets	Customer receives an update within 1 working day where a resolution SLA has been breached	90% of total incidents
Request updates	Customer receives an update to at least the resolution times per request type for	90% of eligible incidents

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

	in-progress requests (e.g. update every 3 working days for in-progress Access request)	

Additional KPIs

The Supplier will be required to demonstrate, monthly, that they are meeting the following KPIs (via suitable management information):

- RCA within 3 working days for P1 and P2 incidents
- Report on failed changes or changes causing issues with reasons

Notes

As new technologies are introduced / transitioned to, the FSA reserve the right to introduce new SLAs to reflect these. New SLA's will be mutually agreed between the FSA and the Supplier prior to their introduction.

Additional Performance Monitoring Requirements
Technical Board *(see paragraph 2 of Call Off Schedule B7).* This can be found on the CCS RM3804 webpage. The document is titled Alternative and additional t&c's v4.
Not Applicable

Section D
Supplier response

Suppliers - use this section to provide any details that may be relevant in the fulfilment of the Customer Order

Commercially Sensitive information
Any information that the Supplier considers sensitive for the duration of an awarded Call Off Contract
Click here to enter text.

Total contract value

Crown
Commercial
Service

13

Please provide the total contract value (for the Call Off Initial Period) as detailed in your response to the Customer's statement of requirements. If a Direct Award, please refer to the Price Card as attached to the Supplier's Catalogue Service Offer.

The contract value is capped at £1,200,000 for the initial contract term, covering the monthly service charge and capacity for contract related project work. The FSA and Little Fish UK will agree additional capacity as part of any variations to extend this agreement.

Section E
Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form and the Call Off Terms (together referred to as "the Call Off Contract") for the duration of the Call Off Contract Period.

SIGNATURES

For and on behalf of the Supplier

Name	██████████
Job role/title	████████████████
Signature	████████████
Date	██████████

For and on behalf of the Customer

Name	██████
Job role/title	██████████████████████████
Signature	████████
Date	█████████

CALL OFF SCHEDULE 7: SCHEDULE OF PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Description	Details
Subject matter of the processing	There will be processing of personal data under this contract. As this contract is for the management and delivery of the FSA's Service Desk function, the supplier will have access to personal data to log incidents and requests for the FSA's end users. The supplier will have permission to access user's profiles which may contain personal information but would not view any information unless it was necessary to carry out their duties under the contract. In order to support end users this may cover viewing personal data on devices which may be personal data processed for FSA business or personal data processed by a user for personal reasons.
Duration of the processing	Processing will take place over the duration of the contract. This is due to expire on the 31/08/2024 with an opportunity to extend by another 2 years (+1 +1).
Nature and purposes of the processing	Personal data is processed for the purpose of delivering the Service Desk contract for FSA Personal and staff data is captured and stored in the FSA's ServiceNow system. It is used to log and action incidents and requests from FSA staff. Where data is stored in the FSA's own ServiceNow instance, no destruction of data is required upon the end of this contract.
Type of Personal Data	Staff data stored includes Name, Job Title, Department, staff Number, Grade, Work email and phone number, work location, Company and Manager. Other FSA supplier contact details such as name and email address and phone numbers.

	Any personal data contained on the FSA user profiles or end user devices which is viewed by supplier personnel when supporting the end user.
Categories of Data Subject	Staff, contractors and suppliers.
Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Data in ServiceNow will not be retained by the supplier or third parties. Personal data held by the supplier outside of the FSA infrastructure is required to be destroyed upon contract completion.

Annex A – Specification of Requirements and Little Fish ITT Response.

Statement of Requirements Purpose

The purpose of this document is to detail the business requirements for the provision of our IT Service Desk; a single, central point of contact for circa 1600 individuals (1300 members of staff & 300 contractors and other supplier) to report issues, raise queries and submit requests, and have them answered and actioned.

Our Service Desk partner will be responsible for

- supporting a range of home and multi-located based users, using the FSA-owned ServiceNow instance to log contacts via multiple communication channels, including chat, service portal, email and telephone

- logging, categorising and prioritising all calls, carrying out initial investigations and resolving at first-contact wherever possible, and providing clear and effective communications to FSA users

- co-ordinating the delivery of services provided by multiple suppliers (both internal and external to the FSA) to ensure response times and SLAs are met, escalating when necessary

The successful bidder will be able to demonstrate evidence of providing a successful service desk function to an organisation of similar size (or larger). They will be able to demonstrate an excellent customer service record, proven communication skills, a good working knowledge of our ITSM software (ServiceNow) and a proven track record of successful innovation to improve and maximise efficiencies in the delivery of this function.

FSA operates in an environment where 24/7 support is necessary to ensure availability of services across the full extent of the FSA working day. We cannot rely on in-hours detection of service failures as this has a significant impact on FSA productivity.

Background

The Food Standards Agency is a non-ministerial government department of over 1300 members of staff and 300 contractors and other suppliers with a big vision – to drive change in the food system so that it delivers "food we can trust". As the country has now left the EU, the scale of this challenge cannot be underestimated. More than 90% of food and feed law in the UK currently comes from Europe and our primary goal is to continue to protect public health and UK consumers' wider interest in food.

The context in which we operate has transformed and continues to change at an unprecedented rate. Digital is the primary way we carry out our work, it is key to achieving our ambitions and transforming the way we do business and we continually strive to

provide better online services to external stakeholders and internal customers to achieve faster and more effective models of delivery at optimal cost.

Our Digital services are supported by a number of specialist delivery partners providing Data Centre Hosting, End User Compute, Service Desk, Wide Area Network, LAN, Application Support, Telephony and Videoconferencing. At the heart of that arrangement is an internal team with the knowledge of our business, our systems and our obligations to enable them to integrate and manage the quality of our services. Key to the success of this multi-vendor model is Support Partner willingness and commitment to work in partnership, collaborating autonomously with other third-party suppliers within a culture of trust and shared goals.

The current disaggregated contract model has been in place since 2017 and as the composite contracts are approaching their maximum term, the FSA has taken the opportunity to review and reconfigure the structure of our contracts and ensure our specifications align with business needs. The output of this review can be found in the FSA's Evergreen IT Roadmap document [**See** FSA30637_015 ODD IT Evergreen Technology Roadmap] which sets out our revised service groupings and our core principles for future digital service development, delivery and support.

Our goal is to be 'evergreen', perpetually updating and improving our services, continuing to adapt to business and political change and adopting new technologies as they emerge. We look to our support partners to be equally flexible and innovative in their approach to delivery, with a strong focus on continuous improvement and quality of service. One of the key benefits of a multi-vendor model is the opportunity to work with specialist suppliers, we want to be guided by expert advice and encourage our support partners to make recommendations based on their experience and a shared desire to improve and evolve.

FSA Transparency

The Agency is committed to openness, transparency and equality of treatment to all support partners. As well as these principles, for science projects the final project report will be published on the Food Standards Agency website (**www.food.gov.uk**).

In line with the Government's Transparency Agenda which aims to encourage more open access to data held by government, the Agency is developing a policy on the release of underpinning data from all of its science- and evidence-gathering projects. Underpinning data should also be published in an open, accessible, and re-usable format, such that the data can be made available to future researchers and the maximum benefit is derived from it. The Agency has established the key principles for release of underpinning data that will be applied to all new science- and evidence-gathering projects which we would expect support partners to comply with. These can be found at **http://www.food.gov.uk/about-us/data-and-policies/underpinning-data**.

Commercial Approach

FSA will complete Premarket engagement on 18th February 2021 (Pre-market Engagement meeting to be held on 12th February 2021 @11am)

FSA are looking to award a contract term for 3 years with 2 separate 1 year optional extensions (i.e. 3+1+1), subject to satisfactory performance. The maximum contract duration is 5 years.

As part of this tender process FSA will not publish finances relating to existing actuals of the incumbent supplier or approved budget for 21/22. FSA will require the Support Partner to develop monthly costs for the supporting information that will be provided with the Tender.

Cost Model

In order to align with our 'Evergreen' goals FSA are looking to our support partner to be flexible and innovative in their approach to the cost model for this tender. FSA are deliberately not being prescriptive here so that the support partner, as the subject matter expert, can be creative in their response and provide a flexible charging model that drives savings over the lifetime of the contract.

The detail provided in section 5 of this document provides all the information and metrics required to produce a comprehensive costing model. FSA requires the support partner to take into account changes to services and how they will work with FSA to a mutually beneficial outcome whilst adding value to the service provision.

The commercial criteria used by FSA to score this element of the tender is as follows:

SCORE	DESCRIPTION FOR SCORE OF THE CRITERIA
100%	There is full justification for the levels of staffing and the overall resources are appropriate. The tender is the best value for money for the work proposed to meet the specification advertised
80%	There is some justification for the levels of staffing and the overall resources requested. The tender is reasonable value for money for the work proposed to meet the specification advertised.
60%	Limited rational is given for the resources requested and/or the tender does not offer very good value for money, but is not poor value
30%	The tender is relatively poor value for money with little/no justification for costs or resources requested

RM3804 Order Form v4 - August 2019

Therefore, the score will be based on value for money assessment not a formula.
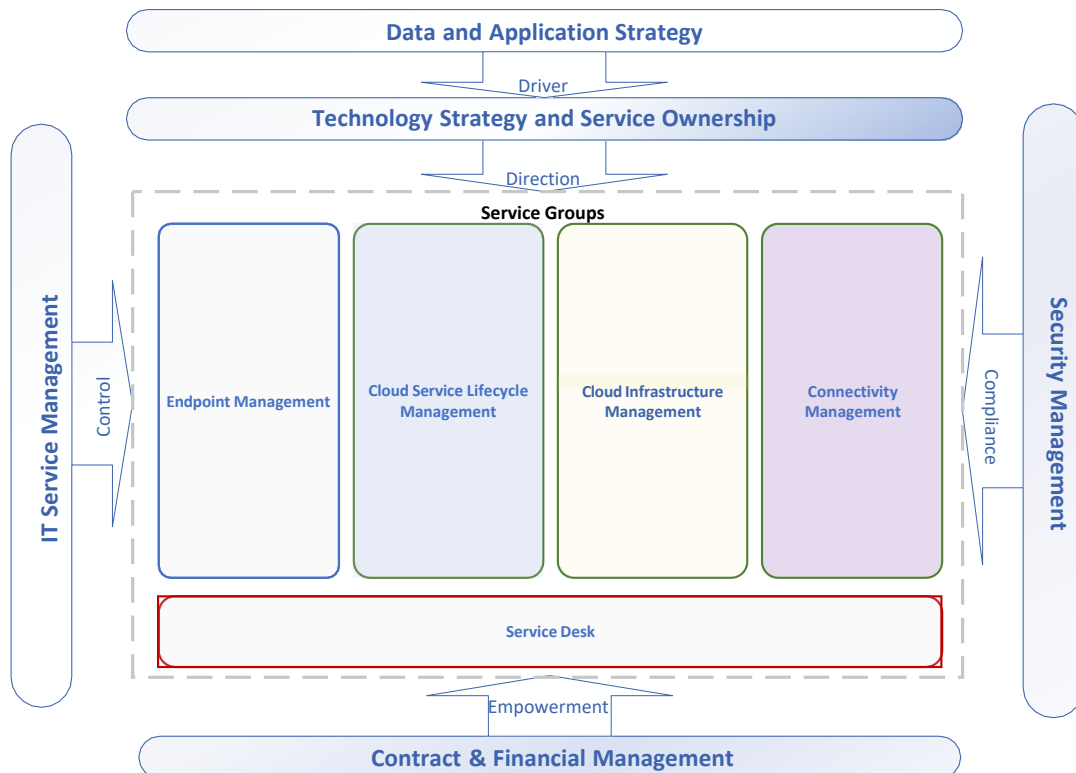
TUPE

TUPE applies and there is a potential that there will be a transfer of staff(s) from the incumbent supplier to the new supplier.

The document [**See** FSA430637_019 Staff Template – TUPE] contains all the information necessary to enable tenderers to submit a tender which takes account of their prospective liabilities.

General Specification

This group of services sits within the overall IT Governance architecture below:

Endpoint Management (Awarded)	**What do we provide?** Ensure that users of FSA IT are provided with the devices and endpoint software required to do their job and that this is properly secured, managed and when necessary replaced.
Cloud Service Lifecycle Management (Released to market)	**What do we use it to do?** Focusses on maintaining application spaces and containers, development tools, but the primary focus is on enabling FSA to make the best use of cloud service offerings and, in particular, to facilitate and implement application migration from server-based IaaS to Platform and Software services.
Cloud Infrastructure Management (Awarded)	**Where do we keep it?** The maintenance and improvement of those data storage services. Management of the overall Azure tenant architecture, it's subscriptions, resource groups, service monitoring, security and reporting and enabling functionality to extend or be replicated across multi-cloud environments. Responsibility also sits here for maintaining the FSA's test and development environments
Connectivity Management (In evaluation phase)	**How do we get to it?** FSA requirements have moved on from the traditional corporate LAN/WAN infrastructure to prioritise the ability to connect to Office 365, Azure and other Cloud Services from any location.
Service Desk (This tender)	**Who do I call when it breaks?** Service Desk is critical the day to day support for end users, but equally manages the toolset for capturing, storing and managing service information. This will continue, alongside a strategic aim to automate workflows and encourage increasing user self-service through a growing knowledge base and increased use of artificial intelligence tools in support of this

In Scope

The following high-level areas are in scope:

1. Service Portal, contact management and communications
2. Incident management

3. Major incident management
4. Request management
5. Knowledge base management
6. Problem management
7. Change management

Out of Scope

1. Hardware and software purchases. These are dealt with under a separate contract.
2. ServiceNow application, support, maintenance, and licenses. The FSA have their own ServiceNow instance which is supported and maintained.

Constraints

1. Due to Covid-19 emergency restrictions on occupancy, distancing and travel to our offices, access to our offices is likely to be restricted in the short to medium term.
2. EU Exit took place the 1st January 2021, although not currently causing significant issues, this may ultimately impact on all government departments contracts and supply chains. In particular, there is a greater focus on us to have a clear understanding of where data is geographically held and the geographical location from which it is being managed.

Business Requirements

The FSA requires a support partner to provide management of its IT Service Desk; a single, central point of contact for our c 1600 members of staff, contractors and other suppliers to report issues, raise queries and submit requests, and have them answered and actioned.

The support partner will be part of a multi-supplier model, working in collaboration with other support partners and FSA teams. The FSA IT team provides the overall management and strategy for both technical architecture and service management.

The support partner will work with the FSA service management team and other support partners to deliver value to customers, optimise efficiency and ensure continual improvement, working to ITIL principles and ensuring that their practices reflect all aspects of the ITIL service lifecycle.

Service Metrics

FSA currently has approximately 1600 members of staff, contractors and other suppliers, all of whom are currently working remotely or from home. In line with our Ways of Working and Estates strategies it should be assumed that this work pattern will predominate in future.

Service desk ticket volumes

Month	Incidents	Service Requests	Total
Jan-20	1366	322	1688
Feb-20	1498	304	1889
Mar-20	2107	435	2674
Apr-20	1300	288	1627
May-20	857	242	1116
Jun-20	1179	290	1515
Jul-20	1166	304	1496
Aug-20	919	229	1223
Sep-20	1096	246	1374
Oct-20	1048	228	1296
Nov-20	1057	254	1344
Dec-20	1081	288	1215

Service desk resolved 86% of incidents in 2020

Incident contacts

Contact type	Chat Media	Email	Phone	Self service	Infrastructure monitoring alert	Walk-up*
Jan-20	918	101	309	0	0	38
Feb-20	910	121	444	0	87	23
Mar-20	1530	237	227	0	95	18
Apr-20	938	141	143	39	39	0
May-20	611	93	97	17	39	0
Jun-20	798	148	153	42	38	0
Jul-20	759	178	147	56	26	0
Aug-20	551	125	187	41	15	0
Sep-20	674	72	284	38	28	0
Oct-20	710	128	238	52	20	0
Nov-20	674	181	142	36	24	0
Dec-20	644	276	125	18	18	0

Incident created times (Jan to Dec '20)

Time of day	No opened
00:00 - 01:00	22
01:00 - 02:00	12
02:00 - 03:00	1
03:00 - 04:00	18
04:00 - 05:00	12
05:00 - 06:00	49
06:00 - 07:00	165
07:00 - 08:00	561
08:00 - 09:00	1219
09:00 - 10:00	1948
10:00 - 11:00	1939
11:00 - 12:00	1797
12:00 - 13:00	1393
13:00 - 14:00	1294
14:00 - 15:00	1393
15:00 - 16:00	1307
16:00 - 17:00	989
17:00 - 18:00	405
18:00 - 19:00	124
19:00 - 20:00	72
20:00 - 21:00	58
21:00 - 22:00	57
22:00 - 23:00	14
23:00 - 00:00	12

Request contacts

Contact type	Email	Chat / Phone	Self-service
Jan-20	216	99	7
Feb-20	185	102	15
Mar-20	267	148	19
Apr-20	197	64	27
May-20	155	68	19
Jun-20	172	87	31
Jul-20	158	58	87
Aug-20	111	51	67
Sep-20	109	40	96
Oct-20	65	43	120

| Nov-20 | 105 | 32 | 117 |
| Dec-20 | 122 | 42 | 124 |

Request created times (Jan – Dec '20)

Time of day	No opened
00:00 - 01:00	0
01:00 - 02:00	0
02:00 - 03:00	0
03:00 - 04:00	0
04:00 - 05:00	0
05:00 - 06:00	2
06:00 - 07:00	5
07:00 - 08:00	84
08:00 - 09:00	193
09:00 - 10:00	297
10:00 - 11:00	399
11:00 - 12:00	436
12:00 - 13:00	267
13:00 - 14:00	398
14:00 - 15:00	390
15:00 - 16:00	405
16:00 - 17:00	405
17:00 - 18:00	126
18:00 - 19:00	12
19:00 - 20:00	1
20:00 - 21:00	2
21:00 - 22:00	4
22:00 - 23:00	3
23:00 - 00:00	1

End user devices

Type	Total (in use)
Laptops	1363
Android Phones	1324
Tablets	40
iPhones	34

RM3804 Order Form v4 - August 2019

| iPads | 10 |
| Thin Clients | 242 |

Pre-qualification Questions

It is important that the Support Partner can answer yes to all pre-qualifications which are part of the overall tender questions. If the Support Partner is unable to answer yes, then the Support Partner is asked not to respond to FSA's tender. For the purpose of market engagement these are the high-level requirements:

1. The Support Partner will have demonstrable experience of providing service desk support to a similar sized or larger organisation

2. The Support Partner will use FSA's ServiceNow service desk solution as the primary ticketing service and will work with all other disaggregated FSA Support Partners.

3. The Support Partner must be structured and equipped to provide a remote service desk solution

4. The Support Partner must have experience working in a multi-Supplier model. For example, dependant on other Suppliers while those Suppliers also have dependencies on you as our Support Partner.

Crown Commercial Service

Operational Requirements

Service	Requirement
1. Service Portal, contact management and communications	• Respond to incoming contacts for chat, service portal, email and telephone in accordance with Service Level Agreements • Ensure incoming contacts are appropriately categorised (incident, request) and updated • Provide communications to keep end users informed of issues that may affect them, or that may reduce the number of enquiries made by users • Provide a telephone response service, including voice recording of all calls and provision of pre-recorded messages (e.g. information on major incidents) • Provision of live-chat functionality available to all users and able to integrate with the FSA ServiceNow instance • Provision of a remote desktop connection solution
2. Incident management **[See FS430634_008 FSA Incident Management Procedure, FSA430637_017 IT SD Service Level Agreements]**	• Provide the incident management function, taking full responsibility for end-to-end incident management, including logging / categorization, monitoring, escalation, evaluation and resolution of incidents within agreed timescales • Ensure incidents are appropriately logged, with all required fields completed accurately, relevant information included, categorised according to the affected services and prioritised • Carry out immediate resolution wherever possible, and where not conduct further investigation and resolution or referral to other suppliers in a timely manner and in-line with SLAs • Evaluate the quality of an incident record, update outstanding information and confirm with the end-user once an incident record is resolved and ready for closure • Monitor the status of active incidents, ensuring regular customer updates are carried out, and taking measures and escalating as soon as

Crown Commercial Service

Service	Requirement
	• possible where service levels are likely to be breached or where the priority increases • Monitor the categorisation and types of active incidents to look for trends and inform prioritisation • Prioritise and investigate escalations from the FSA IT team
3. Major incident management **[See FS430634_008 FSA Incident Management Procedure]**	• Provide the Major Incident Management function, including a nominated individual for each major incident accountable for managing the incident, orchestrating bridge calls and ensuring the required resources are engaged and relevant stakeholders are informed of progress • Provide regular updates for each major incident in accordance with the agreed levels, including progress of investigation, estimated time for restoration and next scheduled update • Produce a major incident report providing details of the incident including description, impact, timeline, resolution, root cause, future preventative measures
4. Request management **[See FS430634_016 FSA Request Fulfilment]**	• Provide the request management function, taking full responsibility for end-to-end request management, including the fulfilment, execution, monitoring, escalation and evaluation / closure of service requests • Ensure requests are appropriately logged, with all required fields completed accurately, and correctly categorised against the relevant service request model • Monitor the status of active requests, ensuring regular customer updates are carried out, and taking measures and escalating as soon as possible where service levels are likely to be breached • Identify, propose requirements and implement new items for service requests, and for efficiencies in existing service request processes (e.g. automation)

Crown
Commercial
Service

Service	Requirement
	• Prioritise and investigate escalations from the FSA IT team
5. Knowledge base management **[See FS430634_011 FSA Knowledge Management Procedure]**	• Monitor the knowledge bases to ensure content is accurate, up-to-date and reviewed according to the specified end dates • Work with other support partners to populate the knowledge base with content to enable first-time fix wherever possible • Populate user knowledge base with appropriate solutions to promote self-service resolution where possible • Ensure known errors and workarounds are identified from incidents, appropriately documented and updated in the knowledge base
6. Problem Management **[See FS430634_010 FSA Problem Management Process]**	• Provide the problem management function, taking full responsibility for the identification, categorisation, prioritisation, diagnosis, resolution and evaluation / closure of problems. • Provide a named resource to manage the problem management process on behalf of the FSA, including chairing of weekly problem meeting • Ensure problems are identified from trends in incidents / major incidents, appropriately logged, with all required fields completed accurately, categorised according to the affected services and prioritised • Manage problem diagnosis and resolution to ensure progress is timely and that regular updates are provided • Evaluate the quality of a problem record throughout, ensuring all relevant information is included, that known error records are updated and information is shared with other service areas
7. Change Management	• Provide support for change management processes, raising changes for own areas of responsibility and ensuring requests requiring a change are related to them and updated

Service	Requirement
[See FS430634_007 FSA Change Management Procedure]	
8. ITSM Toolset (ServiceNow)	• Conduct all service desk activities using the FSA's ServiceNow instance • Identify opportunities for improvements to the ITSM toolset / processes and where possible provide development resource for enhancements and automation as efficiencies for service desk operations
9. Customer satisfaction	• Routinely survey users to establish satisfaction levels with the service desk offering on an individual ticket basis, providing regular reports / data to the FSA, and ensuring feedback is acted upon
10. Other	• The Service Desk Supplier will be located and operate all services within the boundaries of the United Kingdom and, the Supplier, will provide appropriate premises from which to operate the services

Transformation Requirements

While the Operational Requirements are concerned with the ongoing support of existing services, Transformation focuses on the development of services and changes to technology over the course of the contract. Your responses should address, not the day-to-day support, but how you will work with us implement new technologies, reduce technical debt and enable the services we deliver to continue to transform and improve in line with industry roadmaps and best practice standards

Service	Requirement
1. Service Portal, contact management and communications	• Promote the use of the FSA self-service portal as the primary means of contact and information for IT, encouraging a move away from email and telephone contacts to methods that allow either

Service	Requirement
	first-time fix (live chat) or user-resolution (self-service portal / knowledge base • Work with the FSA to set up and use Agent Workspace on ServiceNow, and enable transition from external chat software to ServiceNow Agent Chat • Work with the FSA to facilitate use of AI technologies to enhance the service offering (e.g. automated chatbots)
2. Incident Management	• Reduce the number of incidents raised by users
3. Major Incident Management	• Work with FSA to implement the major incident management module in ServiceNow
4. Service Catalogue	• Work with FSA and other support partners to review offerings across the service catalogue and develop and implement opportunities to automate request processes
5. Technology Roadmap **(See : TBA at point of tender release)**	• Support and provide technical leadership of projects and programmes to deliver the FSA's Technology roadmap • Work with other support partners to continually improve the technical infrastructure across all Service Groups • Work with FSA, and provide pro-active expertise, to identify opportunities for roadmap development and enhancement resulting from business change and industry innovations. • Enable the above by scheduling quarterly (as a minimum) Technology Review meetings with FSA

Service Requirements

Description	Purpose	Priority
Service Availability	• Availability of services, and the support partner support *provision*, should be on a 24/7/365 basis, including core or 'working' hours 7:00am to 8:00pm Monday to Friday, and non-core 8:00pm to 7:00am Monday to Friday plus weekends and bank holidays	Must
Accessibility	• The support partner shall ensure that all services and documentation meet current WCAG accessibility standards for their area of responsibility	Must
User Access	• The support partner shall adhere to the FSA User Access policy. Role based user access must be supported and integration with Azure AD	Must
GDPR	• The support partner must comply with their responsibilities under GDPR	Must

Description	Purpose	Priority
Service Management [**See** previous procedures as well: FS430634_006 FSA Acceptance Into Service Procedure, FS430634_012 FSA Service Asset & Configuration Mgt Procedures, FS430634_018 FSA Patching Policy Sept 2019 1.1]	• The support partner shall work to the respective FSA processes for Acceptance into Service, Change management, Incident Management, Request Management, Knowledge Management, Problem Management, Service Asset and Configuration Management, and contribute as required for their areas of responsibility • The support partner shall provide high- and low-level design documents for all services and solutions. These must be reviewed and updated on at least an annual basis and following the successful implementation of Changes, in line with the FSA knowledge management process • The support partner shall contribute to the review of services, evaluation, definition, execution and monitoring of CSI initiatives, ensuring these are appropriately recorded and reported against • ITIL principles must be followed • The support partner will work on the FSA ServiceNow instance with respect to all service management processes • The support partner shall participate in a monthly service review and shall report on their own performance, including but not limited to incident, request, change, problem, asset management, Continual Service Improvements, Risk, Security, monitoring, SLA performance, patching and endpoint compliance and any ongoing projects for their areas of responsibility • The support partner will work to Service Level Agreements as specified in the FSA Service Level Agreement document	Must
Ways of working	• The support partner shall collaborate with the relevant FSA groups and other third-party support partners in line with the FSA collaboration charter, as well as participate in any testing and training as required	Must

Description	Purpose	Priority
Support Partner's End User Devices	• The support partner shall ensure that: o FSA Data which resides on an uncontrolled support partner device is stored encrypted through a process agreed with the FSA • Any Device used for FSA data is compliant with NCSC End User Devices Platform Security Guidance	Must
Networking	• The Support partner will ensure that any FSA Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted	Must
Personnel Security	• The support partner shall ensure that all personnel are subject to the appropriate pre-employment checks and any additional vetting / national security vetting clearance as required (Baseline Personnel Security Standard for service desk staff)	Must
Hosting and Location of FSA Data	• The Support partner shall ensure that they and none of their Sub-contractors Process FSA Data outside the EEA (including backups) without the prior written consent of the FSA	Must
Security Incident Management	• For an incident that is categorised as a security incident to follow the security incident management policy in parallel to the IT incident management policy. This means not transferring an incident into problem management without sign off from the security team that the risk to FSA data/services has been sufficiently mitigated. The FSA will work with the supplier to waive SLA's in some circumstances in order to continue incident resolution. • The service desk will be the first port of call for users reporting a data breach or a security incident (cyber, technical, physical or personnel) so the Support Partner shall ensure the service	Must

Description	Purpose	Priority
	desk staff have the capability to identify a security and assess an incident and know what steps to take – training material will be provide as part of the onboarding process.	
Understanding of FSA policies	• The Support Partner shall ensure the service desk personnel understand the relevant FSA policies including Records Management and the Acceptable Use Policy to give advice to users based on FSA policy rather than generic guidance e.g. Microsoft.	Must

Little Fish (UK) Ltd Qualification Responses

Supplier	LITTLE FISH (UK) LIMITED
Supplier Evaluation	Accepted
Acceptance or Rejection Notes	
Section Name	1.1 Service Qualification Questions

Question	Description
1.1.1 1	ITSM Toolset (ServiceNow) - Please confirm that you agree to conduct all service desk activities using the FSA's ServiceNow Instance?

Response
Yes

Question	Description
1.1.2 2	Accessibility - Please confirm that you will ensure that all services and documentation meet WCAG 2.1 AA accessibility standards for their area of responsibility.

Response
Yes

Question	Description
1.1.3 3	Service Availability - Availability of services will be on a 24 hours a day, 7 days a week, 365 days a year basis, except where specified with FSA agreement, and including dedicated support for core / working hours and shared support outside of this. Please confirm you agree to this.

Response
Yes

Question	Description
1.1.4 4	Working Hours - The supplier will provide a 24/7/365 service, including core or 'working' hours 7:00am to 8:00pm Monday to Friday , and non-core 8:00pm to 7:00am Monday to Friday plus weekends and bank holidays. Please confirm you agree to this.

Response
Yes

Question	Description

36

RM3804 Order Form v4 - August 2019

![Crown Commercial Service logo]

1.1.5 5	Security Incident Management - The Supplier will comply with the FSA security incident management policy. All security incidents will be prioritised as a P2 or above. Please confirm you agree to this.

<div align="right">Page 2 of</div>

Report run from: Report Area, at: 25/05/2021 10:59

Response
Yes

Question	Description
1.1.6 6	Resource - The supplier will proved a named Service Delivery Manager. Please confirm you agree to this.

Response
Yes

Section Name	1.2 Security Qualification Questions

Question	Description
1.2.1 1	Networking - The Supplier will ensure that FSA Data which needs to be transmitted over networks (including the Internet, mobile networks or un-protected enterprise network, mobile device) shall be encrypted when transmitted. This includes any FSA data held by the Supplier in their own environment. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.2 2	Personnel Security - All Supplier Personnel will be subject to a pre-employment check before they participate in the provision and or management of this Service. Such pre-employment checks must include the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. Please confirm you agree to this.

Response
Yes

RM3804 Order Form v4 - August 2019

Question	Description
1.2.3 3	Personnel Security - The Supplier will work with FSA to determine if any roles that require additional vetting and a specific national security vetting clearance. Roles which are likely to require additional vetting include system administrators whose role would provide those individuals with privileged access to IT systems. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.4 4	Identity, Authentication and Access Control - The Supplier will ensure the access control regime of Service Now ensures all users and administrators are uniquely identified and authenticated when accessing or administering the Services. Please confirm you agree to this.

Page 3 of

Report run from: Report Area, at: 25/05/2021 10:59

Response
Yes

Question	Description
1.2.5 5	Identity, Authentication and Access Control - The Supplier will abide by NCSC best practice and the FSA policy for password creation and reset. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.6 6	Event Logs, Reporting and Protective Monitoring - The Supplier shall ensure service desk personnel can understand and react in line with FSA policy to any security alerts that are received e.g. a risky logon alert. Please confirm you agree to this.

Response
Yes

Question	Description

RM3804 Order Form v4 - August 2019

![Crown Commercial Service logo]

1.2.7 7	Hosting and Location of FSA Data - The Supplier shall ensure that they and none of their Sub-contractors Process FSA Data (including data used in the management of the service in their own system) outside the EEA (including backups) without the prior written consent of the FSA. The Supplier must also provide the locations within the EEA where data is stored. Please confirm that Data would be hosted within the EEA and unless express permission is granted to the contrary.

Response
Yes

Question	Description
1.2.8 8	Vulnerabilities and Patching - the Supplier shall ensure service desk personnel understand the FSA patching policy and what to do if the security team raise a security patching incident with service desk. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.9 9	Malicious Software - If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of FSA Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency. Please confirm you agree to this.

Response

Page 4 of

Report run from: Report Area, at: 25/05/2021 10:59

Response
Yes

Question	Description
1.2.10 10	Secure Architecture - The Supplier will ensure services are designed in accordance with the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main; Please confirm you agree to this.

Response

RM3804 Order Form v4 - August 2019

Yes

Question	Description
1.2.11 11	Secure Architecture - The Supplier will ensure services are designed in accordance with the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.12 12	Secure Architecture - The Supplier will ensure services are designed in accordance with the NCSC "End User devices", a copy of which can be found at https://www.ncsc.gov.uk/collection/end-user-device-security. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.13 13	Secure Architecture - The supplier will ensure services are designed in accordance with the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles. Please confirm you agree to this.

Response
Yes

Question	Description
1.2.14 14	Principles of Security - The Supplier shall be responsible for the confidentiality, integrity and availability of FSA data whilst it is under the control of the Supplier and consequentially the security of the system/service. Please confirm you agree to this.

Response
Yes

Page 5 of

Report run from: Report Area, at: 25/05/2021 10:59

Question	Description

RM3804 Order Form v4 - August 2019

1.2.15 15	Certification - the Supplier has Cyber Essentials PLUS. Please confirm you hold this certification.
Response	
Yes	

Question	Description
1.2.16 16	Assurance - the Supplier will create an information Security Management Document Set to document how they will comply with the specific FSA security requirements to be approved by the Head of Security at the FSA. Please confirm you agree to this.
Response	
Yes	

Question	Description
1.2.17 17	Incident and Breach Management - reporting - If the Supplier becomes aware of a Breach of Security covering FSA data including on their own systems (including a Personal data breach) the Supplier will inform the FSA at the earliest opportunity. Please confirm you agree to this.
Response	
Yes	

Little Fish (UK) LTD Operational Response

TENDER	FS430637 - SERVICEDESK

Section 1: Service Portal, contact management and communications – 15%

A Respond to incoming contacts for chat, service portal, email and telephone in accordance with Service Level Agreements.

Q1 - How will you ensure that the specified communication channels are appropriately resourced to meet the response SLAs required? – 20%

B Ensure incoming contacts are appropriately categorised (incident, request) and updated.

Q2 - How will you ensure contacts are categorised accordingly, and how might the process of creating incidents / requests from contacts be improved? – 10%

[REDACTED]

C Provide communications to keep end users informed of issues that may affect them, or that may reduce the number of enquiries made by users.

Q3 - Describe your approach to user communications, and how these would reduce / prevent the number of enquiries / tickets raised by users? – 20%

[REDACTED]

D Provide a telephone response service, including voice recording of all calls and provision of pre-recorded messages (e.g. information on major incidents)

Q4 - Describe your telephone response service, and how you would ensure it is available on a 24/7/365 basis? – 20%

E Provision of live-chat functionality available to all users and able to integrate with the FSA ServiceNow instance

Q5 - Describe the live-chat function you would use and how this will be integrated with the FSA's ServiceNow instance – 20%

44

F Provision of a remote desktop connection solution.

Q6 - Describe the remote desktop connection solution you would recommend – 10%

Section 2: Incident management – 25%

A Provide the incident management function, taking full responsibility for end-to-end incident management, including logging / categorization, monitoring, escalation, evaluation and resolution of incidents within agreed timescales.

Q7 - Describe your approach to incident and major incident management, and how you would identify and resolve incidents for your areas of responsibility. Please feel free to include any diagrams/process flows into your answer – 20%

Crown
Commercial
Service

[REDACTED]

B Ensure incidents are appropriately logged, with all required fields completed accurately, relevant information included, categorised according to the affected services, prioritised and where relevant assigned correctly.

Q8 - Describe how you achieve this, what steps you will take to ensure incident ticket quality is maintained and how other resolvers receive the right information – 15%

[REDACTED]

Crown
Commercial
Service

47

C Carry out immediate resolution wherever possible, and where not conduct further investigation and resolution or referral to other suppliers in a timely manner and in-line with SLAs.

Q9 - How do you ensure that incidents are resolved immediately whenever possible? – 15%

D Evaluate the quality of an incident record, update outstanding information and confirm with the end-user once an incident record is resolved and ready for closure.

Q10 - What checks do you undertake before closing an incident? – 10%

49

E Monitor the status of active incidents, ensuring regular customer updates are carried out, and taking measures and escalating as soon as possible where service levels are likely to be breached or where the priority increases.

Q11 - How do you ensure that customers always receive timely updates for your own and other suppliers' incidents? What actions would you take to prevent service levels breaching for your own and other suppliers' incidents? – 15%
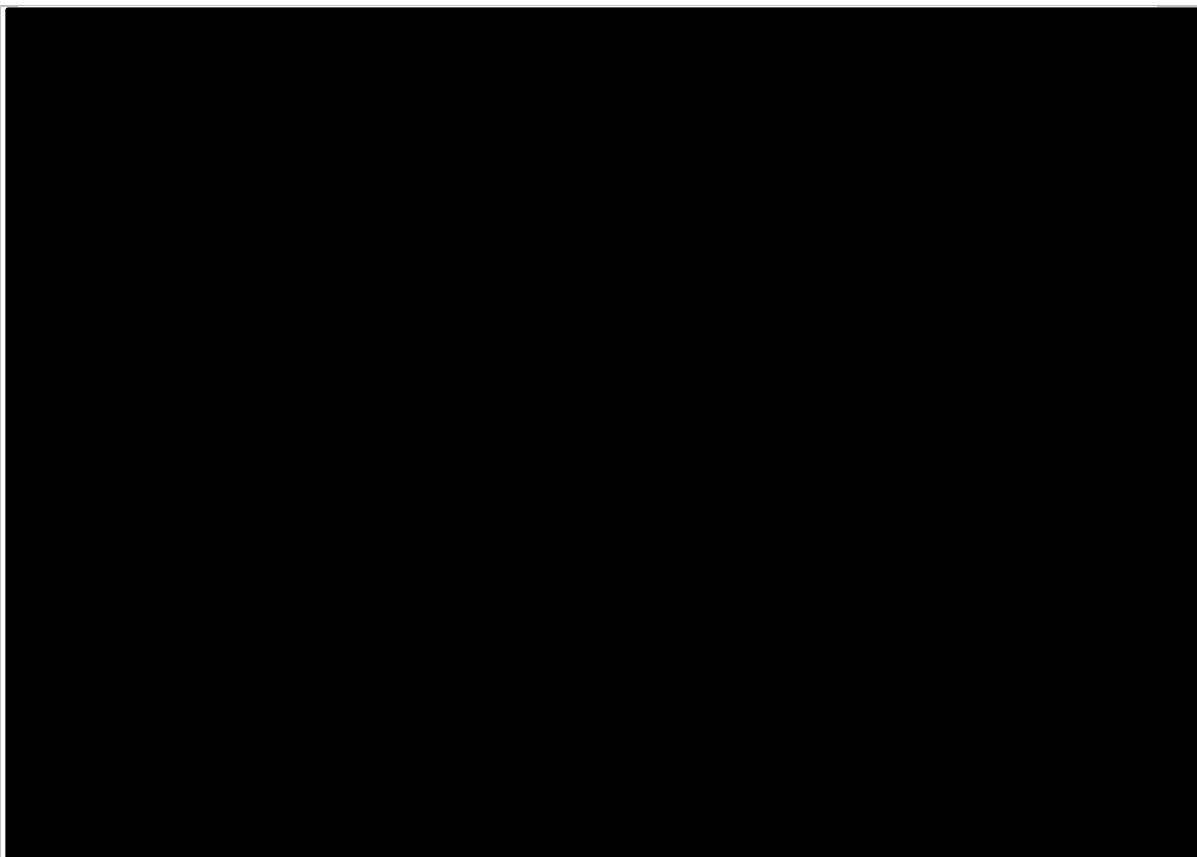
F Monitor the categorisation and types of active incidents to look for trends and inform prioritisation.

Q12 - What monitoring would you undertake on active incidents and why? – 15%

G Prioritise and investigate escalations from the FSA IT team

Q13 - The FSA IT team, in particular the service team, are an internal point of escalation - how would you ensure incidents and issues relating to incidents raised by this team were prioritised and that you take responsibility for updating customers? – 10%

Section 3: Major incident management – 9%

A Provide the Major Incident Management function, including a nominated individual for each major incident accountable for managing the incident, orchestrating bridge calls and ensuring the required resources are engaged and relevant stakeholders are informed of progress.

Q14 - Describe your approach to major incident management, and how you will ensure resource is available when required on a 24/7/365 basis. Please feel free to include any diagrams/process flows into your answer – 40%

Crown
Commercial
Service

███

███

███

███

B Provide regular updates for each major incident in accordance with the agreed levels, including progress of investigation, estimated time for restoration and next scheduled update.
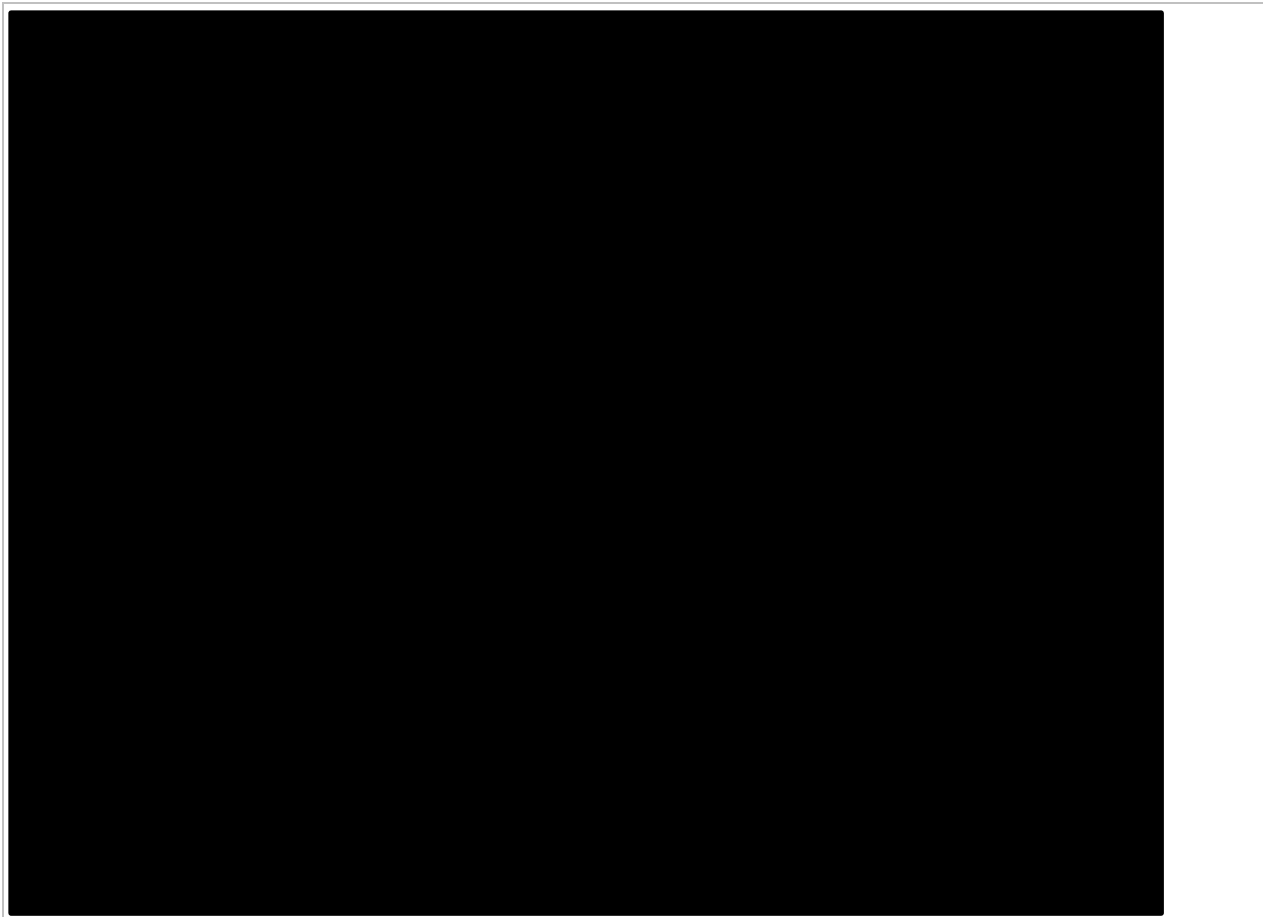
Q15 - Describe how you will provide updates to relevant stakeholders in a major incident scenario - 30%

███

███████████████████████████████████

54
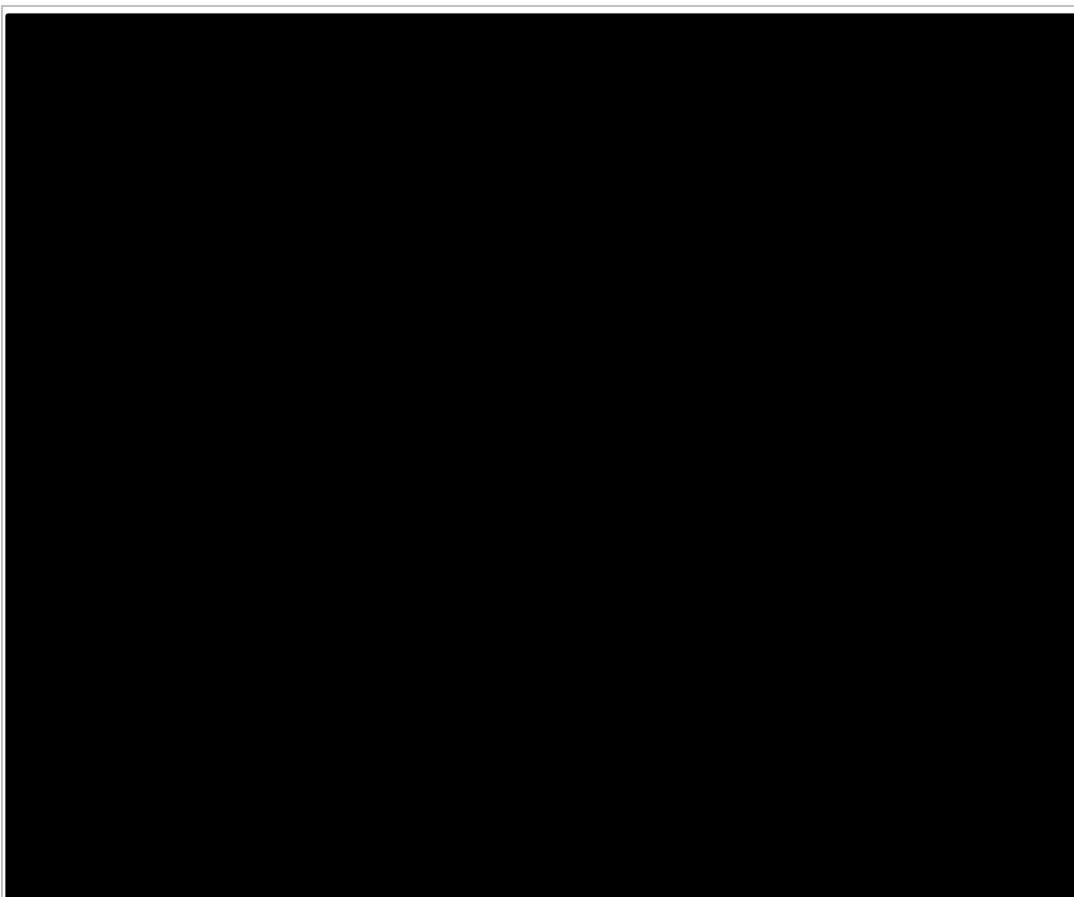
C Produce a major incident report providing details of the incident including description, impact, timeline, resolution, root cause, future preventative measures.

Q16 - What information do you include in major incident reports and why is this important? – 30%
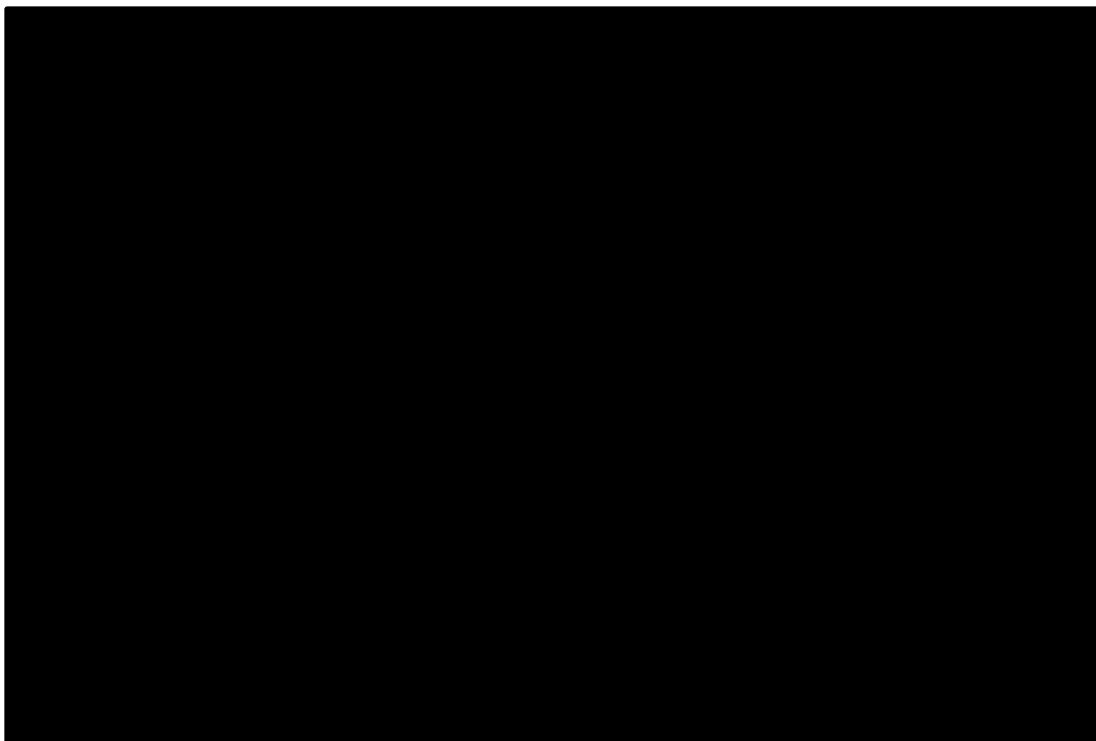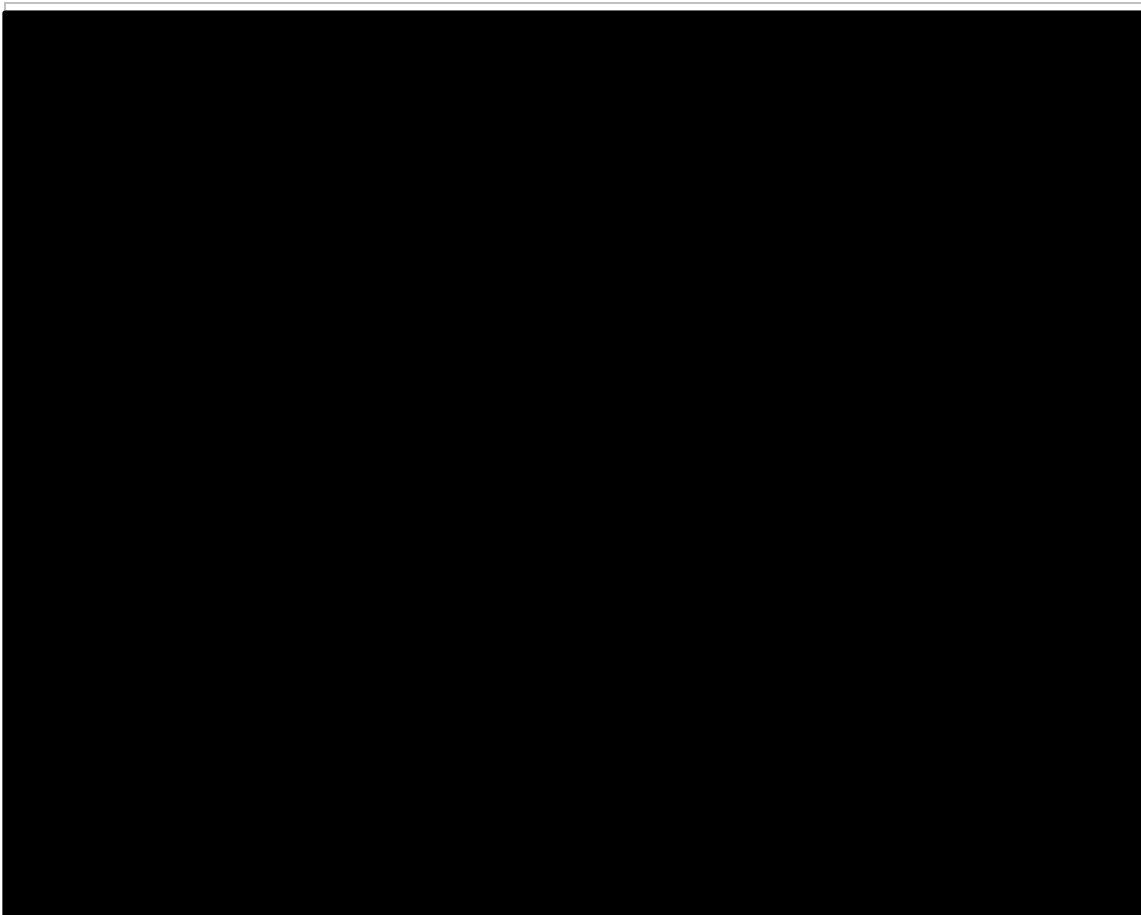
Section 4: Request management – 20%

A Provide the request management function, taking full responsibility for end-to-end request management, including the fulfilment, execution, monitoring, escalation and evaluation / closure of service requests.

Q17 - Describe your approach to request management and how you ensure these are monitored and managed to achieve customer satisfaction. Please feel free to include any diagrams/process flows into your answer – 40%
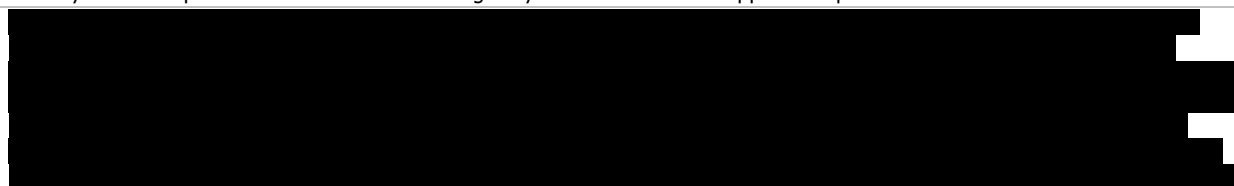

B Ensure requests are appropriately logged, with all required fields completed accurately, and correctly categorised against the relevant service request model.

Q18 - Describe how you achieve this, what steps you will take to ensure request ticket quality is maintained and how other resolvers receive the right information – 10%

C Monitor the status of active requests, ensuring regular customer updates are carried out, and taking measures and escalating as soon as possible where service levels are likely to be breached.

Q19 - How do you ensure that customers always receive timely updates for your own and other suppliers' requests? What actions would you take to prevent service levels breaching for your own and other suppliers' requests? – 20%

[Crown Commercial Service logo]

██

██

D Identify, propose requirements and implement new items for service requests, and for efficiencies in existing service request processes (e.g. automation).

Q20 - How would you identify new items suitable for service requests? Please provide an example of process efficiencies you have made for service requests – 20%

██

██

██

██

E Prioritise and investigate escalations from the FSA IT team.

Q21 - The FSA IT team, in particular the service team, are an internal point of escalation - how would you ensure issues relating to requests raised by this team were prioritised and that you take responsibility for updating customers? – 10%

[Crown Commercial Service logo]

[redacted content]

Section 5: Knowledge base management – 10%

A The supplier shall work to the FSA knowledge management process, and contribute to the production of, analysis, timely review and sharing of knowledge and information in the FSA's Knowledge Base. The supplier is responsible for ensuring the knowledge base is up-to-date and accurate for the services they support.

Q22 - Describe your approach to knowledge management. Please feel free to include any diagrams/process flows into your answer – 30%

[redacted content]

B Monitor the knowledge bases to ensure content is accurate, up-to-date and reviewed according to the specified end dates.

Q23 - How would you monitor the FSA ServiceNow knowledge base to ensure these checks were undertaken? – 20%

C Work with other support partners to populate the knowledge base with content to support a 'shift-left' approach and enable first-time fix wherever possible.

Q24 - How would you identify, recommend and implement opportunities to enable first-time fixes? - 20%
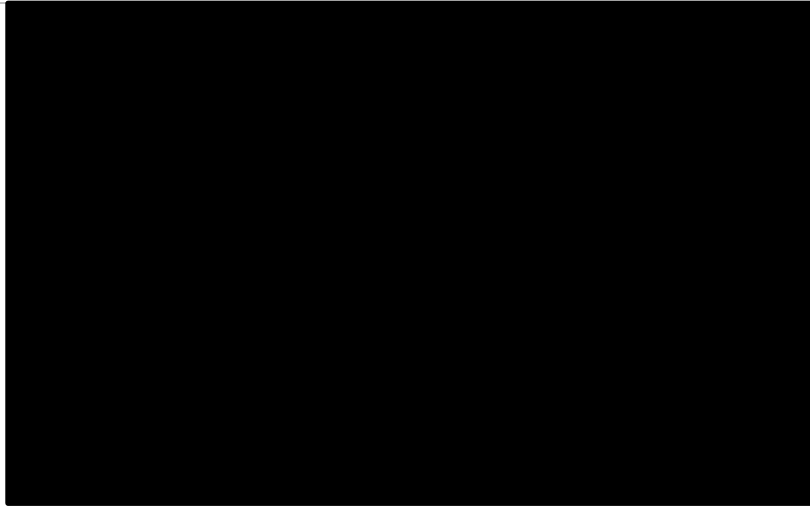
D Populate user knowledge base with appropriate solutions to promote self-service resolution where possible.

Q25 - How would you identify and update user knowledge to promote self-service resolution? How might you monitor the effectiveness of this? - 20%

E Ensure known errors and workarounds are identified from incidents, appropriately documented and updated in the knowledge base.

Q26 - How would you ensure known-errors and workarounds were identified and added to the knowledge base? – 10%
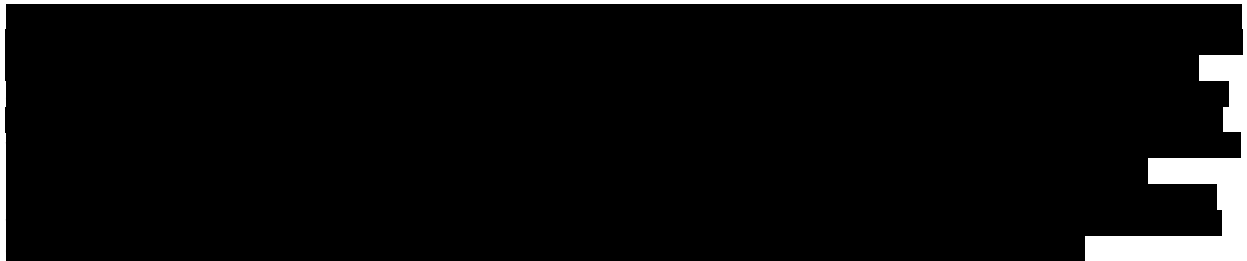
Section 6: Problem management – 10%

A Provide the problem management function, taking full responsibility for the identification, categorisation, prioritisation, diagnosis, resolution and evaluation / closure of problems.

Q27 - Describe your approach to problem management. Please feel free to include any diagrams/process flows into your answer – 30%

RM3804 Order Form v4 - August 2019
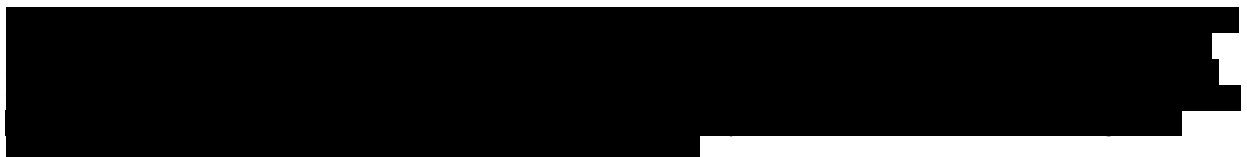
B Provide a named resource to manage the problem management process on behalf of the FSA, including chairing of weekly problem meeting.

Q28 - Describe your experience of providing problem management for other organisations – 30%

C Ensure problems are identified from trends in incidents / major incidents, appropriately logged, with all required fields completed accurately, categorised according to the affected services and prioritised.

Q29 - How would you identify new problem records and that these are recorded and updated accurately? – 15%

[Crown Commercial Service logo]

D Manage problem diagnosis and resolution to ensure progress is timely and that regular updates are provided.

Q30 - Describe your experience of driving problem resolution in a disaggregated service model – 10%

E Evaluate the quality of a problem record throughout, ensuring all relevant information is included, that known error records are updated and information is shared with other service areas.

Q31 - How will you ensure that the quality of problem records are maintained and that timely updates are provided? – 15%

Section 7: Change management – 1%

A The supplier shall work to the FSA change management process, and contribute to the assessment, logging, review, implementation, scheduling, review and closure of changes.

Provide support for change management processes, raising changes for own areas of responsibility and ensuring requests requiring a change are related to them and updated.

Q32 - Describe your approach to change management and what actions you take to minimize the risks associated with changes. Please feel free to include any diagrams/process flows into your answer – 100%

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

65

[content redacted]

Section 8: ITSM Toolset (ServiceNow) – 5%

A Identify opportunities for improvements to the ITSM toolset / processes and where possible provide development resource for enhancements and automation as efficiencies for service desk operations.

Q33 - Describe your experience in identifying and implementing improvements to ITSM toolset processes – 100%

[content redacted]

[Crown Commercial Service logo]

[Redacted content]

Section 9: Customer satisfaction – 5%

A Routinely survey users to establish satisfaction levels with the service desk offering on an individual ticket basis, providing regular reports / data to the FSA, and ensuring feedback is acted upon.

Q34 - How will you monitor and manage customer satisfaction for the FSA? – 100%

[Redacted content]

2. [Redacted content]

67

Little Fish (UK) Ltd Transformational Response

TENDER REFERENCE	FS430637 - SERVICEDESK

Section 1: Service Portal, contact management and communications – 50%

A Promote the use of the FSA self-service portal as the primary means of contact and information for IT, encouraging a move away from email and telephone contacts to methods that allow either first-time fix (live chat) or user-resolution (self-service portal / knowledge base).

Q1 - What steps would you take to increase uptake of the FSA self-service portal and to encourage use of the preferred contact methods? – 50%

B Work with the FSA to set up and use Agent Workspace on ServiceNow and enable transition from external chat software to ServiceNow Agent Chat.

Q2 - Describe your experience of using and/or migrating to Agent Workspace and Agent Chat on ServiceNow – 10%

RM3804 Order Form v4 - August 2019

C Work with the FSA to facilitate use of AI technologies to enhance the service offering (e.g. automated chatbots).

Q3 - Give an example/s of your use of AI technologies to enhance a service offering – 40%

Section 2: Incident Management - 20%

A Reduce the number of incidents raised by users.

Q4 - How would you reduce the number of incidents raised by users? – 100%

Crown
Commercial
Service

Section 4: Service Catalogue – 15%

A Work with FSA and other support partners to review offerings across the service catalogue and develop and implement opportunities to automate request processes.

Q6 - Provide examples of any request processes you have successfully automated – 100%

Section 5: Technology Roadmap – 10%

A Support and provide technical leadership of projects and programmes to deliver the FSA's Technology roadmap.

Q7 - Describe your approach to project delivery and how you will provide technical leadership to cross-supplier project teams – 10%

B Work with other support partners to continually improve the technical infrastructure across all Service Groups.

Q8 - FSA is seeking suppliers who continually improve their service offering and embed this into existing services. Describe how you have provided in-service improvements over the past two years, as part of business as usual operations, for a customer similar to the FSA – 80?

74
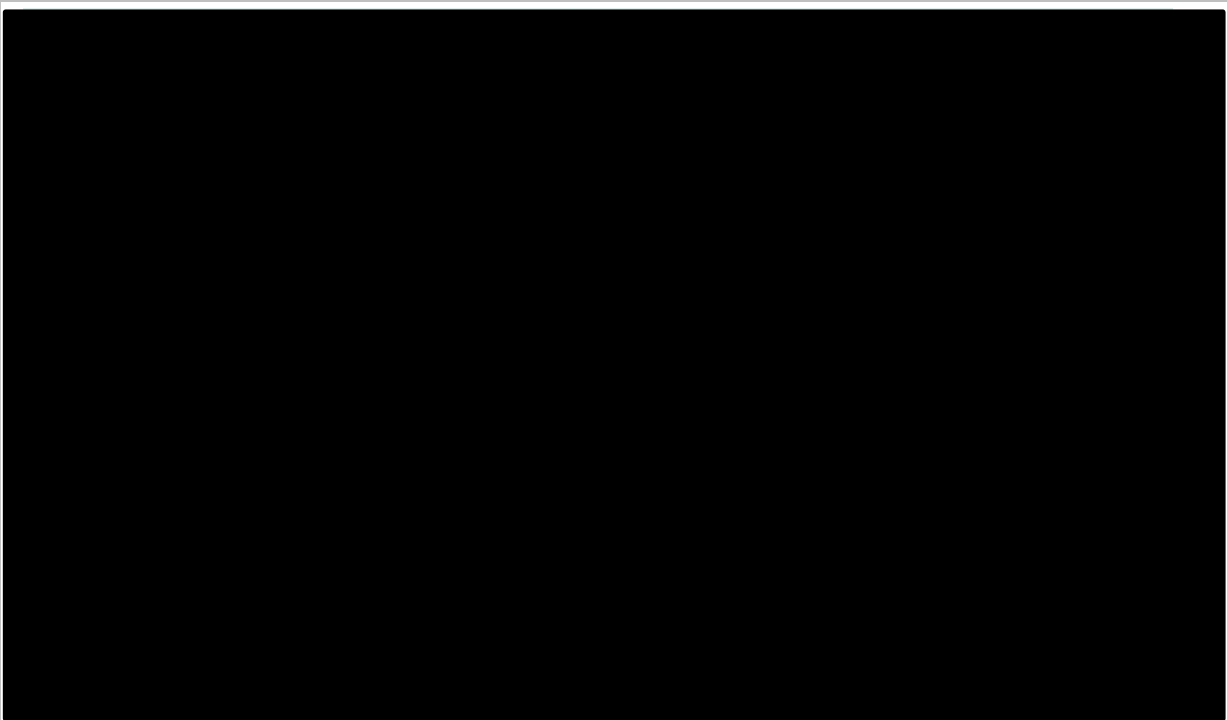
C Work with FSA, and provide pro-active expertise, to identify opportunities for roadmap development and enhancement resulting from business change and industry innovations.

Q9 - How will you support the FSA's Technology Roadmap and provide pro-active expertise, to identify opportunities for roadmap development and enhancement resulting from business change and industry innovations? – 10%

RM3804 Order Form v4 - August 2019

76

Little Fish (UK) Ltd Service Response

TENDER REFERENCE	FS430637 - SERVICEDESK			

Section 1: Service Management – 45%

A Monitoring - The supplier will provide performance monitoring and reporting for any services under its area of responsibility, ensuring issues are identified and investigated and working with the FSA to resolve as required.

Q1 - Describe how you would use monitoring and reporting to proactively identify outages and degradation of services, and ensure appropriate action is taken to limit the impact on end-users – 10%

B Acceptance into Service - The supplier shall work to the FSA Acceptance into Service process and contribute to the provision and assessment of all relevant requirements specified for any new services.

Q2 - Describe your own processes for the acceptance of new services, and how these ensure you are able to provide appropriate support. Please include your own process flows/diagrams in your answer – 18%

RM3804 Order Form v4 - August 2019

RM3804 Order Form v4 - August 2019

C Monthly Service Review - The supplier shall participate in a monthly service review and shall report on their own performance, including but not limited to incident, request, change, problem management, Continual Service Improvements, Risk, Security, monitoring, SLA performance and any ongoing projects for their areas of responsibility. The report must be submitted to FSA 5 working days from the start of the new month.

Q3 - Explain your approach to monthly performance reports and how you would highlight issues or areas of concern – 20%

D Service Asset and Configuration Management - The supplier shall work to the FSA Service Asset and Configuration Management process and contribute to the definition and maintenances, mapping of interrelationships, appropriate control and verification / audit of configuration items.

Q4 - Describe your approach to configuration management and how you would contribute to identification and updates of configuration items and dependencies. Please feel free to include any diagrams/process flows into your answer – 5%

RM3804 Order Form v4 - August 2019
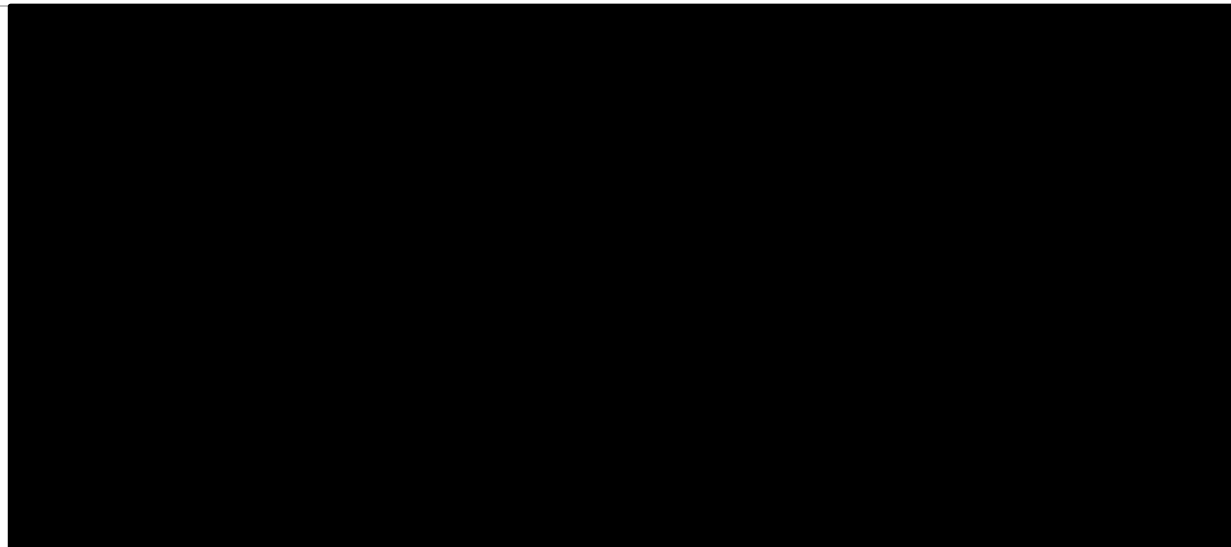
E Customer Satisfaction - The FSA will seek customer satisfaction feedback, the supplier is expected to contribute to drafting of surveys, act upon negative feedback or declining rates of satisfaction, and include initiatives to improve satisfaction levels in their CSIP.

Q5 - Describe your approach to the analysis of customer satisfaction feedback, and how you would use these findings to improve service quality – 20%

F Business Continuity

Q6 - In the event that the FSA invokes Business Continuity plans the supplier will work with the agency to understand how it can best support operational continuity.

RM3804 Order Form v4 - August 2019

Please confirm you agree to this – Yes/No response – 1%
Yes
Q7 – The supplier will provide up to date Business Continuity plans for their organisation on an annual basis Please confirm you agree to this – Yes/No response – 1%
Yes
Q8 - The supplier shall ensure that service is delivered to the FSA in the event of further pandemic lockdowns or local tier-based restrictions. Describe your approach to delivery of the required Service Desk services in a pandemic lockdown scenario – 5%
██

G Service Level Agreements - The supplier will work to Service Level Agreements as specified in the FSA Service Level Agreement document.

Q9 - Explain how you will manage, monitor and achieve the expected performance criteria specified in the FSA SLA document – 20%

██

82

Section 2: Continuous Service Improvement – 5%

A Continual Improvements - The supplier will provide contractual wide continuous improvement ensuring that all aspect of technology, service and commercial are identified, reviewed, recommended and improved throughout the lifecycle of the contract.

Q10 - Explain how you will achieve this requirement and provide examples which have resulted in quality improvements or monetary savings – 100%

Crown
Commercial
Service

84

Section 3: Ways of Working – 15%

1.   A Collaboration - The supplier shall collaborate with the relevant FSA groups and the FSA's other third-party suppliers as required. This is a key principle of the disaggregated service delivery model and must be appear seamless to the end user.

Q11 - Describe your experience of working with a range of different suppliers and how you are able to integrate successfully with them – 15%

Q12 - Describe your collaborative approach to complex or major incident management in a disaggregated service delivery model – 15%

85

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

███
████████████████████

██
██

██
██
██
███████████████████

██
██
███████████████████████

██
██

██
██

B Testing - The supplier will be expected to participate in appropriate testing for any services that is within their responsibility.

Q13 - Describe your approach to testing for new services related to Service Desk that you use and / or support – 5%

██
██
████████████████████████████

C ITIL Principles - ITIL principles must be followed.

Q14 - Describe how you ensure your staff have an appropriate understanding of ITIL principles – 1%

██
██

██
██

██
██

██
███████████

Crown
Commercial
Service

Q15 - Describe how you will ensure your staff members adopt and understand FSA's policies and procedures – 14%

D Resource - It is the suppliers responsibility to identify and supply key personnel across the service offering (including projects) to maintain service levels and availability of escalation points.

Q16 - Explain how you plan to resource this service offering, detailing key personnel and escalation routes – 45%

- ████████████████████ line management support to the POD of Service Desk Engineers. Also responsible for; ensuring delivery of agreed service levels and improve the quality of the service desks work

[black redaction blocks]

- [black redaction block]

E Compatibility - The supplier shall ensure that any services and applications for their areas of responsibility are consistent with FSA technology stack and can be used by FSA IT staff, resolver groups, other suppliers and end users where appropriate.

Q17 - Describe how you will ensure the services you provide are consistent with FSA technology stack and Evergreen principles – 5%

[black redaction blocks]

Section 4: Project Management – 1%

A Project process

Q18 - The supplier will provide flexibility in project process and deliver using either an agile or waterfall technique depending on the type of project.

Please confirm you agree to this – Yes/No response – 50%

Yes

RM3804 Order Form v4 - August 2019

B Project Services.

Q19 - The Supplier will provide Project management services for delivery of transformation, ongoing development and implementations across suppliers.

Please confirm you agree to this – Yes/No response – 50%

Yes

Section 5: Security – Personnel Security – 2

A Personnel Security:

Requirement 1 - All Supplier Personnel will be subject to a pre-employment check before they participate in the provision and or management of this Service. Such pre-employment checks must include the HMG Baseline Personnel Security Standard including verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

Requirement 2 - The Supplier will work with FSA to determine if any roles that require additional vetting and a specific national security vetting clearance. Roles which are likely to require additional vetting include system administrators whose role would provide those individuals with privileged access to IT systems.

Q20 – The Supplier shall not permit Supplier Personnel who fail the security checks required by the first two requirements (above) to be involved in the management and/or provision of the Services except where the FSA has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
Please confirm you agree to this - Yes/No response – 40%

Yes

Q21 - The Supplier shall ensure that Supplier Personnel are only granted such access to FSA Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

Please confirm you agree to this - Yes/No response – 30%

Yes

Q22 – The Supplier will ensure that any Supplier Personnel who no longer require access to the FSA Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the FSA Data revoked within 1 Working Day.

Please confirm you agree to this – Yes/No response – 30%

Yes

Section 6: Security – Identity, Authentication and Access Control – 6%

A Identity, Authentication and Access Control:

Q23 – The Supplier will provide reports/data on the records of access to the System/Service e.g. Service Now to the FSA on request.

Please confirm you agree to this – Yes/No response – 30%

Yes

Q24 – The Supplier will comply with the FSA access policy for access to FSA Systems/Services.

Please confirm you agree to this – Yes/No response – 50%

Yes

RM3804 Order Form v4 - August 2019

Q25 - The Supplier will they comply with the FSA principle to use Multi- Factor Authentication.

Please confirm you agree to this – Yes/No response – 20%

Yes

Section 7: Security - Event Logs, Reporting and Protective Monitoring – 8%

A The Supplier will produce monthly reports which document the security incidents raised. The parameters of these reports are to be agreed with the security team but will include the details of the incident action taken and trends

Q26 - How would you present the data and trend analysis in a format that can be readily shared with the FSA Board and business community for assurance (non-technical audience) – 50%

Q27 - In order to facilitate effective monitoring the Supplier will interface with other FSA Suppliers to contribute to regular reports setting out (as a minimum) changing access trends, any unusual patterns of usage and traffic, risky logins malicious or suspicious activity on the network. The reports will also cover action the Supplier took in raising a ticket for either an incident or problem or event and the outcome.

Please confirm you agree to this – Yes/No response – 40%

Yes

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

Q28 - The FSA receives a monthly threat surface report and the supplier will undertake to resolve any vulnerabilities and issues this identifies in the service for which they are responsible.
Please confirm you agree to this – Yes/No response – 10%
Yes

Section 8: Security - Vulnerabilities and Patching – 6%

A Vulnerabilities and Patching

Q29 - The Supplier undertakes to keep Systems where FSA data resides on their own environment patched and up to date in line with NCSC best practice.
Please confirm you agree to this – Yes/No response – 100%
Yes

Section 9: Security – Certification – 1%

A The Supplier is certified to ISO/EC 27001:2013 by a UKAS approved certification body or included in the scope of an existing certification of compliance of ISO/IEC 27--1:2013.

Q30 - Pease confirm - Yes/No response – 100%
Yes

Section 10: Security Testing: IT Health Check – 1%

A The Supplier will co-operate with the FSA annual IT Health Check and project specific tests by a CHECK IT supplier and be responsible for implementing any actions assigned to them in the resulting remedial action plan.

Q31 - Pease confirm you agree to this - Yes/No response – 100%
Yes

Section 11: Security – Assurance – 4%

A Assurance

Q32 - The Supplier will provide copies of their data protection security patching, protective monitoring, access and security policies to the FSA.
Pease confirm you agree to this - Yes/No response – 20%
Yes
Q33 - The Supplier will work with the FSA to complete a Personal Data Processing Statement as part of the contract.
Pease confirm you agree to this - Yes/No response – 30%
Yes
Q34 - The Supplier will work with the FSA to mitigate any risks assigned to them in the Privacy Impact Assessment if applicable.
Pease confirm you agree to this - Yes/No response – 20%
Yes
Q35 - The Supplier will notify the FSA immediately if they identify a new risk to the components or architecture of the system/service that could impact the security of FSA data, a change in threat profile or proposed change of site.

Pease confirm you agree to this - Yes/No response – 30%

Yes

Section 12: Security – Compliance Audits – 4%

A Compliance Audits

Q36 - The Supplier will support compliance with security assurance audit activity carried out by FSA against these requirements see link https://www.gov.uk/government/publications/government-supplier-assurance-framework.

Pease confirm you agree to this - Yes/No response – 100%

Yes

Section 13: Incident and Breach Management – reporting – 2%

A The Support Partner shall ensure the service desk personnel understand the relevant FSA policies including Records Management and the Acceptable Use Policy to give advice to users based on FSA policy rather than generic guidance e.g. Microsoft.

Q37 - Can you describe your understanding of why government departments need to manage information and comply with Acceptable Use policies and the risks of not doing either of these things properly – 25%

Q38 - For an incident that is categorised as a security incident to follow the security incident management policy in parallel to the IT incident management policy. This means not transferring an incident into problem management without sign off from the security team that the risk to FSA data/services has been sufficiently mitigated. The FSA will work with
the supplier to waive SLA's in some circumstances in order to continue investigating a p1/p2 security incident.

Pease confirm you agree to this - Yes/No response – 25%

Yes

Q39 - The service desk will be the first port of call for users reporting a data breach or a security incident (cyber, technical, physical or personnel) so the Support Partner shall ensure the service desk staff have the capability to identify and assess an incident and know what steps to take – training material will be provided as part of the onboarding process.

Pease confirm you agree to this - Yes/No response – 50%

Yes

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

Little Fish (UK) LTD Commercial Response

TENDER	FS430637 - SERVICEDESK

Section 1: On-boarding Cost – 10%

A To demonstrate that the supplier has a full understanding of any potential onboarding costs.

Q1 – Please provide a breakdown of onboarding costs that your organisation anticipates – 100%

Section 2: Flexible Charging 70%

A It is a core goal of FSA to continuously optimise all services and therefore the supplier must be able to quickly react to changes.

Q2 - Please provide your suggested cost model for the service outlined in the document FSA430637_001 Service Desk Specification V2 - Section 5. Include a breakdown of your workings and demonstrate how the costs may be flexibly changed in line with changes to the service. The response should determine how the supplier will instigate savings and efficiencies for the duration of the contract.

Section 3: Change Management – 10%

A In some cases FSA may want to perform a change to the contract to reflect changes in technology innovation. This is part of FSA's core principle of Evergreen.

Q3 - Can you explain how your organisation will drive innovation using change and if there are any commercial thresholds to such a change. Include how instigating a change to contract will affect charges over the duration of the contract – 100%

Section 4: Project Activity – 5%

B FSA are keen to understand the suppliers definition of a Business As Usual verses project activity.

Q4 - Can you supply your definition and any threshold between Business As Usual and project activity – 100%

2)

[REDACTED]

Section 5: Early Termination 5%

A FSA are keen to understand the suppliers position on early termination costs.

Q5 - Can you supply details of what early termination costs you would expect FSA to pay if the contract was terminated for convenience? Include the level of any caps on any amounts payable to the supplier – 100%

[REDACTED]

Section 6: Rate Card - 0% (this is not part of the scored evaluation but for the FSA's reference

A Rate Card

Q6 – Please provide your project rate card, to help the FSA understand potential project costs over contract lifetime – 0%

RM3804 Order Form v4 - August 2019

Crown
Commercial
Service

POST TENDER CLARIFICATIONS

PROJECT REFERENCE : FS430633
PROJECT TITLE : Service Desk

Date : 16 July 2021

Between: The Food Standards Agency (the Authority) and Little Fish (UK) Ltd (the Contractor)

1. The Tender is revised as follows:

Clarification/Revision 1:

Requirement	Query	Action required	Littlefish Answer
Operational Section 6 A: Provide the problem management function, taking full responsibility for the identification, categorisation, prioritisation, diagnosis, resolution and evaluation / closure of problems.	Answers to operational q's 27 – 31 describe process and experience of problem management but the resource (Service Q16) doesn't include a problem manager.	Confirm that problem management resource as described in answers 27 - 31 is included and will take full ownership of the process	ITIL v4 Problem Management resource will be appropriately aligned to the FSA account and take full ownership of the Problem Process
Operational Section 1 C: Provide communications to keep end users informed of issues that may affect them, or that may reduce the number of enquiries made by users	Littlefish response to Q3: "We recommend that FSA retains ownership of issuing communications to users, while working together with the Littlefish Service Desk, Change Management and Major Incident Management functions to ensure accuracy and consistency of messaging"	Confirm that Littlefish will take responsibility for issuing communications to users as required, subject to appropriate mechanisms being in place	Confirmed. Where appropriate LF's MIM resource will sense check communication content with the FSA, but would create and issue the communication. LF are conscious that all Service communication is being sent on FSA's behalf
Operational Section 2: Incident Management Provide the incident management function, taking full responsibility for end-to-end incident management, including logging / categorization, monitoring, escalation, evaluation and resolution of incidents within agreed timescales.	Answer to Q7 focuses on Incident Management, details of Major Incident Management process and required activities not described. Answers to Q9, 12 & 13. Insufficient detail, lack of ownership and intervention from an incident manager described	Provide Littlefish MI process and confirm LF will take full ownership of process, details of required activities can be agreed at onboarding	An ITIL v4 Major Incident Management resource will be appropriately aligned to the FSA account and take ownership of the MIM Process. See email attachment "LF-SMO-Major Incident Management Swimlane Process v1.1.pdf"
Operational Section 2 Incident management A To G	Incident Manager referenced in some answers, e.g. Q8: "design a component in ServiceNow which will randomly pick tickets within the tool to be reviewed by the Incident Manager"; Q12: "These notifications trigger the Incident Manager to review the incident and either ensure	Confirm that an incident manager will be part of the allocated resource and available in core hours to receive escalations, monitor ticket quality, manage SLAs and carry out trend analysis	ITIL v4 Incident Management resource will be appropriately aligned to the FSA account during core hours. Typically Trend Analysis is the responsibility of Problem Management

97

	the engineer/owner has everything" but the resource (Service Q16) doesn't include the incident management provision.		
Operational Section 3 A: A Provide the Major Incident Management function, including a nominated individual for each major incident accountable for managing the incident, orchestrating bridge calls and ensuring the required resources are engaged and relevant stakeholders are informed of progress.	Answers to operational q's 14 – 16 describe process and experience for major incident management but the resource (Service Q16) doesn't include the major incident management provision.	Confirm that major incident management resource as described in answers 14 - 16 is included, both in and outside of core hours	Confirmed
Operational Section 4: Request management	Answers to Q18 & 19 are missing significant detail around how LF will monitor ticket quality, provide updates to the requestor and manage 3rd party supplier requests	Confirm resource allocated to fulfil these requirements, available during core hours to action escalations and drive fulfilment. Detail of required activities can be agreed at onboarding	ITIL v4 Request Management resource will be appropriately aligned to the FSA account during core hours.
Operational Section 5 Knowledge base management A to E (all requirements)	"The Littlefish Knowledge Management function will work cross-functionally not only with the Service Desk, but also other resolver groups across the Service Ecosystem". The resource (Service Q16) doesn't include this provision	Confirm that LF will own the knowledge management function, owning the process for management of the KB, monitoring and maintaining accuracy and driving reviews across the ecosystem	Confirmed
Service Section D: Resource - It is the suppliers responsibility to identify and supply key personnel across the service offering (including projects) to maintain service levels and availability of escalation points.	Service desk personnel not included in response, but is part of current provision and referenced in Operational Q1: "Continuing today's model, we propose to retain a dedicated Service Desk Pod for FSA that provides the benefit of known agents that are not only familiar with FSA's users but also the technical and business environments"	Confirm service desk resource	At the current time approximately 4 full time ServiceDesk associates are aligned to FSA's dedicated POD. There is also overflow provision which will vary on demand (intra-day).

Commercial Section 2: Flexible Charging Q2 - Please provide your suggested cost model for the service outlined in the document FSA430637_001 Service Desk Specification V2 - Section 5. Include a breakdown of your workings and demonstrate how the costs may be flexibly changed in line with changes to the service. The response should determine how the supplier will instigate savings and efficiencies for the duration of the contract.	The response provides a cost based on 'per ticket' but also quotes a 'per user' cost. It's not clear how this will work in practice.	Clarify details of how the fixed costs and flexible charging (per user) will be achieved. Do the fixed costs show what FSA would expect to pay monthly and then the flexible costs would be reviewed at agreed milestones?	The service is priced per user based on the volumes provided in the ITT.

The fixed costs show what FSA would expect to pay monthly and the flexible costs are to provide both parties a fair use policy to trigger a flex up or down.

Part of monthly reporting is to collate volumes and that data feeds the bi-annual review. I.e. should a flex up or flex down be considered based on the data in-hand and the ratios (0.8 and 1.1) beingbreached or not.

Both parties agree that the calculation for an increase or decrease in charging will be discussed at 6 month milestones (based on a review of user numbers and ticket volumes over the past 6 months). The commitment to an annual reduction in charges will be agreed at the annual contract review. |
| Commercial Section 4: Project Activity - Q4 - Can you supply your definition and any threshold between Business As Usual and project activity | Project Activity is called out in three Tiers. Tier 1 indicates that a Service Introduction Manager resource would be required. In the current contract this type of activity is covered by the SDM. | Confirm why additional resource is required (outside of BAU) for a tier 1 activity. | On reflection and in the spirit of partnership, LF accepts that any small or minor Service Introduction performed by Service Desk staff should be treated as BAU and not Project. |

Response (if required):

2. The Technical and Commercial Submission shall remain effective and unaltered except as amended by this Agreement these documents shall be used to form the contract.

3. Unless and until directed otherwise, nothing in this document, shall be construed as giving a guarantee of any remunerative work whatsoever unless or until such work is requested and confirmed by means of a duly authorised Purchase Order.

4. Until a Purchase Order is received from the Agency, you should not assume that the sum requested will be granted, that the project will not require modification, or that the project will commence on the starting date requested.

Signed:

RM3804 Order Form v4 - August 2019

For the Authority

Signature: ██████████████

Name: ████████████

Title: ██████████

Date: ████████

For the Contractor

Signature: ██████████████

Name: ██████████

Title: ████████████████

Date: ██████████

100

ANNEX B – Work Package Template

FS430637
Request for Quotation

Work Package Number:	
Work Package Title:	
Available Budget: £	
Supplier Name: Little Fish (UK) LTD	
Specification of requirements – (to be completed by FSA)	
Supplier response – please provide a detailed methodology of how you will deliver the requirements	
Delivery timescales – Please provide a detailed plan of when you will deliver the specified outcomes	
Please detail any assumptions you have made	
Please detail any identified risks and your proposed mitigation measures	
Costings – Please provide a detailed breakdown of all costs to deliver the specified requirements	
GDPR - Processing, Personal Data and Data Subjects (where not covered by overarching contract)	

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with the overarching contract, (Where the Party is a Controller and the other Party is Processor) 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:

RM3804 Order Form v4 - August 2019

	• *[Insert the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
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	*[Describe how long the data will be retained for, how it be returned or destroyed]*
Completed by:	
Date:	

Date quotation accepted by FSA:
Work Package start date:

This quotation for the above mentioned Work Package has been agreed between the Food Standards Agency and the Supplier under the terms and conditions of the contract FS430637 – ServiceDesk

Signed on behalf of the FSA

Name:

Signature: --

Position:

Date:

Signed on behalf of the Supplier

Name:

Signature: --

Position:

Date:

RM3804 Order Form v4 - August 2019