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
Clive House, 70 Petty France, Westminster, London, SW1H 9EX

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

Customer representative contact details
Email and telephone contact details for the Customer's representative
[redacted]

Supplier details

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

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

[redacted]

Supplier representative contact details
Email and telephone contact details of the supplier's representative
Telephone number – [redacted]
Email Address - [redacted]

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

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)

1. TECHNOLOGY STRATEGY & SERVICES DESIGN ☐
2. TRANSITION & TRANSFORMATION ☐
3. OPERATIONAL SERVICES

a: End User Services ☒

b: Operational Management ☐

c: Technical Management ☐

d: Application and Data Management ☐

4. PROGRAMMES & LARGE PROJECTS

a. OFFICIAL ☐

a. SECRET (& above) ☐

Customer project reference
Please provide the customer project reference number.

FS430633

Call Off Commencement Date

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

31/08/2021

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 Months

Call Off Extension Period (Optional) Months
24 Months (2 X 12 month extensions)

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
FS430633_006 FSA Acceptance Into Service Procedure
FS430633_007 FSA Change Management Procedure
FS430633_008 FSA Incident Management Procedure
FS430633_009 FSA Security Incident Procedure 2019
FS430633_010 FSA Problem Management Process
FS430633_011 FSA Knowledge Management Procedure
FS430633_012 FSA Service Asset & Configuration Mgt Procedures
FS430633_013 FSA Supplier Access Policy August 2019 v1
FS430633_014 FSA IT Acceptable Use Policy Nov 2020 v3.2
FS430633_016 FSA Request Fulfilment
FS430633_018 FSA Patching Policy Sept 2019 1.1

FS430633_006 FSA Acceptance Into Servi
FS430633_007 FSA Change Management
FS430633_008 FSA Incident Management
FS430633_009 FSA Security Incident Proc
FS430633_010 FSA Problem Managemen
FS430633_011 FSA Knowledge Managem
FS430633_012 FSA Service Asset & Confi
FS430633_013 FSA Supplier Access Policy
FS430633_014 FSA IT Acceptable Use Policy
FS430633_016 FSA Request Fulfilment.do
FS430633_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.

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

Additional Clauses and Schedules

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). ☒

A3: Staff Transfer

A4: Exit Management

A: PROJECTS - Optional

A1: Testing □

A2: Key Personnel ☒

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

B1: Business Continuity and Disaster Recovery ☒

B2: Continuous Improvement & Benchmarking ☒

B3: Supplier Equipment

B4: Maintenance of the ICT Environment □

B5: Supplier Request for Increase of the Call Off Contract Charges □

B6: Indexation □

B7: Additional Performance Monitoring Requirements □

Optional Clauses
Can be selected to apply to any Order

Tick any applicable boxes below

C: Call Off Guarantee □

D: Relevant Convictions □

E: Security Requirements ☒

F: Collaboration Agreement
Where required please complete and append to this Order Form as a clearly marked document (see Call Off Schedule F) □

G: Security Measures □

H: MOD Additional Clauses □

Alternative Clauses

To replace default English & Welsh Law, Crown Body and FOIA subject base Call Off Clauses

Tick any applicable boxes below

Scots Law □
Or

Northern Ireland Law □

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	**Third Party Software**
Click here to enter text.	Datto Software

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
- FSA Devices and peripherals held in stock by the supplier in order to provision equipment to end users. This includes, but is not limited to, laptops, tablets, mobile phones, sim cards.
- FSA Devices and peripherals held by the supplier whilst awaiting disposal.
- Any Devices shared with the supplier to enable them to carry out aspects of the contract, such as testing device.

Call Off Contract Charges and Payment Profile *(see Call Off Schedule 2)*
Include Charges payable by the Customer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)

On-Boarding Costs:
[redacted]

Initial Monthly Costs:
[redacted]

Payments will be made by BACS, monthly in arears. Invoices will be submitted to accounts-[redacted] with a copy sent to [redacted]

Undisputed Sums Limit (£) *Insert right (see Call Off Clause 31.1.1)*	[redacted]
Delay Period Limit (calendar days) *Insert right (see Call Off Clause 5.4.1(b)(ii))*	NA

Estimated Year 1 Call Off Contract Charges (£) [redacted]
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)*

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.*	This will be agreed between the FSA and Little Fish. based on the high-level transition plan included in the ITT response.

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

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

List below or append as a clearly marked document to include Key Roles

Customer Service Director
Service Account Manager
Service Delivery Manager
Head of Infrastructure and Operations

Customer Responsibilities

List below or append as a clearly marked document

Click here to enter text.

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)
Please see relevant Personnel Security questions in ITT qualification envelope and Technical Envelope.

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 8:01pm to 6:59am 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.

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….):

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	1 hour from assignment of issues	8 hours for critical services,	No more than 1 failure

	unit experiencing significant reduction in system performance.		8 working hours for non-critical services	
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 than 2 failures
P4	Minor disruption: single user or user group experiencing problems, but with circumvention available	1 working day from assignment of issue	3 working days	

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

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

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
Provision of a device (laptop, mobile, tablet, thin-client), from the point of request to delivery to the user – except	5 working days	90% or no more than 2 failures

where the device is a priority replacement device (see below)		
Provision of a priority replacement device (i.e. the user's current main device is not functional and they are unable to work), from the point of request to delivery to the user	2 working days	90% or no more than 2 failures
Packaging and distribution of applications through distribution tools such as MS Company portal and FSA's Play, Apple and Microsoft Stores.	3 working days	90% or no more than 2 failures

Device 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

Description	Target to be achieved in month
Operating Systems are maintained at N-1	100%
Operating systems are patched on at least a monthly cycle and devices maintained at N-1 for functional patches and updates	100%

Additional KPIs

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

- Any supported hardware or software approaching end of life or end of support is identified
- 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 – 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
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 £1,800,000 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	[redacted]
Job role/title	[redacted]
Signature	[redacted]
Date	[redacted]

For and on behalf of the Customer

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

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 endpoint devices and software, the supplier, their third-party subcontractor, and courier service will have access to personal data to deliver and collect devices, such as laptops, tablets and phones, as well as specialist software. The supplier will have access to users' local copies of OneDrive, which may contain personal information but would not view any information within a OneDrive unless it was necessary to carry out their duties under the contract. In order to support the endpoint devices this may cover viewing personal data on the device which may be personal data processed for FSA business or personal data processed by a user for personal reasons. One example is checking for malware on the device There may also be processing of personal data associated with the service of providing backups.
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 endpoint contract for FSA Personal and staff data is captured and stored in the FSA's ServiceNow system and provided in Excel sheets for the purpose of managing, delivering and collecting devices for staff while working remotely from home. It is also used to log and action requests for staff equipment and specialist software. The supplier, their third-party subcontractor or the courier will be required to contact the person directly to facilitate device/asset delivery. Where data is stored in the FSA's own ServiceNow Instance, no destruction of data is required upon the end of this contract. However, the supplier will be required to operate projects on behalf of the Agency, where personal data will be provided outside of the FSA infrastructure.
Type of Personal Data	Name, home address, personal email address, personal phone number. 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 end user devices which is viewed by supplier personnel when supporting the devices.
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 or third parties outside of the FSA infrastructure is required to be destroyed upon project completion.

Annex A – Specification of Requirements and Little Fish (UK) Ltd ITT response.

Statement of Requirements Purpose

The purpose of this document is to detail the business requirements for the provision of Endpoint Management, the operation and continual improvement of the end to end processes of issuing both desktop and mobile IT equipment to our c 1300 members of staff. This includes support, patching and update of client and server operating systems and for virtual as well as physical desktops.

The Food Standards Agency (FSA) has transformed our ways of working to become a primarily home and multi-location based organisation and, while Covid-19 has accelerated this, our expectation is that this progression will continue in the long term, with fewer staff using office space and on a less frequent basis. Our Endpoint Management partner will, therefore, be able to offer an efficient service for issuing new and replacement devices to users with a range of connectivity methods across England, Wales and Northern Ireland, enabling a straightforward user experience with an increasing focus on self-service, particularly around software downloads.

Your response should also address how you will be able to support our developing client and application virtualisation services centred on Windows Virtual Desktop (WVD) and potentially support the integration of this with increased use of users' own devices.

Much of the above will be dependent on the effective use of Microsoft Endpoint Management (aka Intune) as the management tool for both Windows, Android and IOS devices.

FSA operates in an environment where 24/7 management 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 people, 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** FSA30635_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**.

1. Commercial Approach

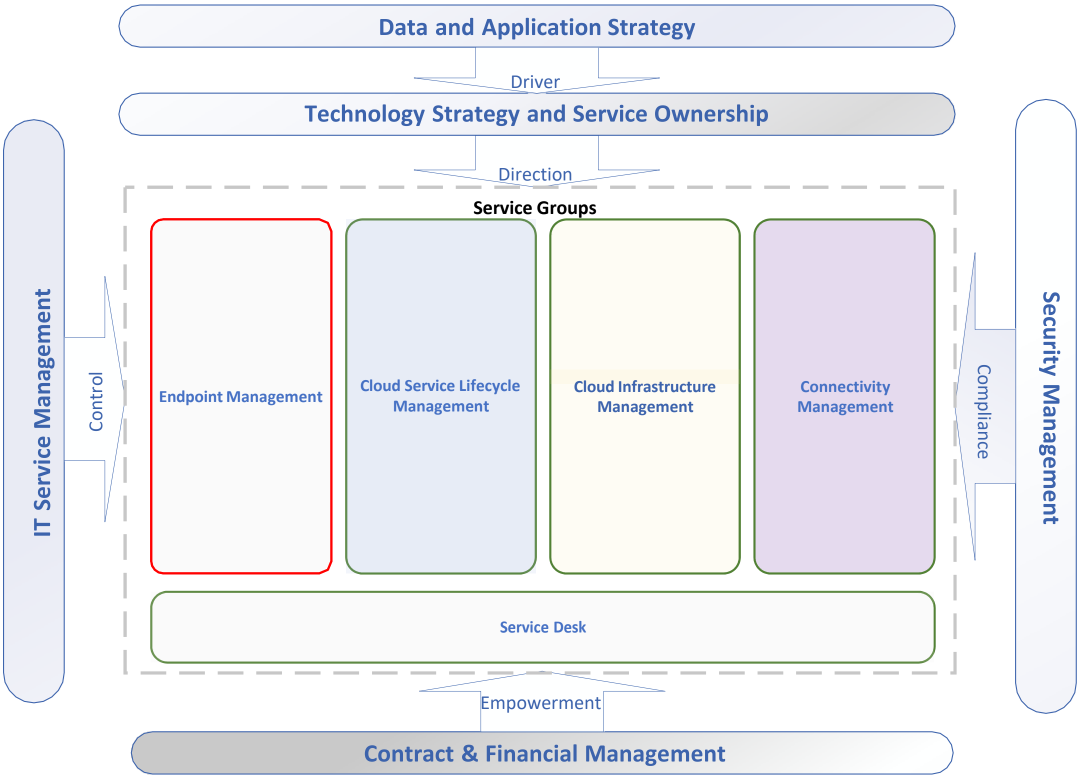
FSA will complete Premarket engagement on 19th November 2020.

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.

General Specification

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


Data and Application Strategy
Driver
Technology Strategy and Service Ownership
Direction
Service Groups
IT Service Management
Control
Endpoint Management
Cloud Service Lifecycle Management
Cloud Infrastructure Management
Connectivity Management
Compliance
Security Management
Service Desk
Empowerment
Contract & Financial Management

Endpoint Management (This Tender)	**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 (Future Tender)	**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 (Out for Tender - CCS RM3804 Technology Services 2 framework, lot 3d)	**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 (Future Tender)	**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 (Future 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

a. In Scope

The following high-level areas are in scope:

1. Store, build, dispatch, manage, maintain, swap out and return of laptops, mobile phones, and tablets
2. Software and Hardware Asset Management
3. Desktop, Server and Mobile Operating Systems
4. Device management (Microsoft Endpoint Management)
5. Endpoint protection and patching
6. Virtual Applications and Desktops
7. Thin Client Devices, Operating Systems and Management Tools
8. Client access to mobile networks – including deployment of SIM cards and 4G routers
9. Management of onsite FSA audio and video conferencing endpoints
10. Print management solution
11. Disposal of equipment

b. Out of Scope

1. Hardware and software purchases. These are dealt with under a separate contract. Peripherals are out of scope for storage. These will be sent directly from our hardware supplier
2. Support for Cloud Environments such as Microsoft 365 and other line of business services is covered by Cloud Service Lifecycle Management. Endpoint Management will be responsible for publishing client, MS store and desktop applications to end users.
3. The provision of a service desk function. This is covered by a separate contract.
4. ServiceNow application, support, maintenance, and licenses. The FSA have their own ServiceNow instance which is supported and maintained.

c. 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 “go-live” is planned for the 1st January 2021, although not expected to cause issues, this may impact on all government departments contracts and supply chains.

Business Requirements

d. Overview

The FSA requires a support partner to provide management of its endpoint devices and device management solutions as part of a cloud first IT Architecture, ensuring the provision of hardware and software across the lifecycle that meets the needs of users in a flexible and mobile-working environment.

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 will provide 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.

e. Service Metrics

FSA currently has approximately 1300 members of staff, 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.

Device totals are as follows:

Type	Total (in use)	Built and deployed avg. pcm	Decomm & disposal avg. pcm	Current FSA Stock Level	Required Maximum level to store
Laptops	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Android Phones	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Tablets	[redacted]	[redacted]		[redacted]	[redacted]
iPhones	[redacted]				[redacted]
iPads	[redacted]	[redacted]		[redacted]	[redacted]
Thin Clients	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Printers (plant and Home)	[redacted]	[redacted]	[redacted]		[redacted]

Windows Server VMs	130	Managed under Change and Project Control	N/A
Linux Server VMs	9		N/A
WVD Host Pools	6		N/A
WVD Application Groups	16		N/A
Physical Windows Servers (Hyper-V hosts)	5		N/A

Type	Device Make & Model	OS Level	In use	In stock
Laptop	Lenovo T470s (type 20HF, 20HG) Laptop (ThinkPad) - Type 20HG	Windows	[redacted]	[redacted]
Laptop	Lenovo T480s (type 20L7, 20L8) Laptop (ThinkPad) - Type 20L8	Windows	[redacted]	[redacted]
Laptop	Lenovo T490s (Type 20NX, 20NY) Laptop (ThinkPad) - Type 20NX	Windows	[redacted]	[redacted]
Laptop	Lenovo T490s (Type 20NX, 20NY) Laptop (ThinkPad) - Type 20NY	Windows	[redacted]	[redacted]
Laptop	Lenovo X260 Laptop (ThinkPad) - Type 20F5	Windows	[redacted]	[redacted]
Laptop	Lenovo X260 Laptop (ThinkPad) - Type 20F6	Windows	[redacted]	[redacted]
Laptop	Lenovo Miix 720-12IKB Tablet (ideapad) - Type 80VV	Windows	[redacted]	[redacted]
iPad	Apple iPad Air 2	iOS	[redacted]	[redacted]
iPad	Apple iPad Mini 4	iOS	[redacted]	[redacted]
iPad	Apple iPad Pro (10.5 inch)	iOS	[redacted]	[redacted]
iPad	Apple iPad Pro (11 inch)	iOS	[redacted]	[redacted]
Tablet	Lenovo Tab 10	Android	[redacted]	[redacted]
Tablet	Samsung Galaxy Tab 2	Android	[redacted]	[redacted]
Tablet	Samsung Galaxy Tab A	Android	[redacted]	[redacted]
Tablet	Samsung Galaxy Tab A6	Android	[redacted]	[redacted]
Tablet	Samsung Galaxy Tab A8	Android	[redacted]	[redacted]

Mobile Phone Make and Model	OS	In use	In stock
Samsung A40	Android	[redacted]	[redacted]
Samsung J5	Android	[redacted]	[redacted]
Apple iPhone XR	iOS	[redacted]	[redacted]
Samsung J6+	Android	[redacted]	[redacted]
Apple iPhone 7	iOS	[redacted]	[redacted]
Samsung Galaxy S8	Android	[redacted]	[redacted]

Please note that peripherals will be shipped directly from FSA's hardware supplier and therefore the Support Partner for Endpoint Management will not be expected to provide storage space for these.

f. Pre-Qualification

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 will be asked not to respond to FSA's tender. For the purpose of market engagement these are the high-level requirements provided on 17th November

1. The Support Partner will have demonstrable experience of using Microsoft Autopilot and Endpoint Manager (aka Intune) to manage Windows and Mobile devices.

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 support end user devices in a Remote First organisation with limited use of FSA office space.

4. The Support Partner must provide secure storage at a registered premise for a maximum buffer stock of 180 devices.

5. 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.

Operational Requirements

Service	Requirement
1. Device Provision	• Manage the provisioning of end user devices, including laptops, tablets, thin client devices and mobile phones, for issue to FSA staff. Provisioning must not require staff to attend FSA offices for the issue of equipment or resolution of incidents and requests • Proactive management of the device provision to ensure all staff members devices needs are met without delay • Store and issue a buffer stock of devices, delivered by FSA's hardware suppliers, and issue these direct to users' home or corporate addresses • Be responsible for the replacement and decommission of end user devices, including retrieval from meat premises, corporate offices and from users' home address and storage pending reissue or disposal • Securely dispose of hardware in line with NCSC guidance for Official/Official-Sensitive material
2. Operational Asset Management	• Manage the lifecycle of assets for both hardware and software, ensuring appropriate asset control, management of the asset / CMDB records in ServiceNow, stock and licence management, allocation and distribution of assets through request fulfilment, Audit of asset records to ensure accuracy and compliance, and advising the FSA for planning for replacement of End of Life Assets • Work with FSA to decommission legacy hardware, operating systems and client applications.
3. Operating Systems	• Maintain and support client, mobile and server Operating Systems[1]. This currently includes the following OS: ○ Windows 10, ○ Windows Server,

[1] Clarification: Overall management of the Azure VM estate, including server provisioning, sizing, management of Resource Groups, backup, decommissioning is the responsibility of Cloud Infrastructure Management. Endpoint Management is responsible for ensuring that individual servers are patched and updated to an agreed schedule, are assigned to the correct Active Directory OUs, have malware protection and that performance and events are monitored and alerts actioned.

Service	Requirement
	○ Android, ○ IOS, ○ Red Hat, Ubuntu and CentOS Linux, ○ Microsoft Hyper-V, ○ Wyse Thin-OS, ○ IGEL • OS updates, including Windows 10 Service Channel Updates, will form part of the standard service. Ensure that Operating Systems, are maintained at N-1 and that OS version updates are rolled out across devices on a schedule to meet this requirement. • Ensure that Windows and Linux virtual servers (in the Azure IaaS environment supported by FSA's Cloud Infrastructure Management partner) meet NCSC Baseline Security standards and are patched and maintained at N-1 and that there is a managed regular patching update and malware management schedule • Pro-actively monitor all supported hardware and software for end of life and end of support. Advise FSA of, and initiate, appropriate remedial actions.
4. Device Management Tools	• Manage End User Devices using Microsoft Endpoint Management (aka Intune), • Configure, operate and maintain Device Configuration and Compliance policies, ensuring that devices are configured in line with NCSC guidelines and are managed centrally to ensure ongoing compliance. This includes the remote wipe and reset of compromised or missing devices • Configure, operate and maintain Windows Autopilot, Android Enterprise and Apple Business Manager for device enrolment. • Configure, operate and maintain the packaging and distribution of applications through distribution tools such as MS Company portal and FSA's Play, Apple and Microsoft Stores. • Configure, operate and maintain device management tools for systems not covered by

Service	Requirement
	Microsoft Endpoint Management (e.g. Dell Wyse tools for thin client management) • Maintain and keep updated a standard set of software for download and installation during device setup; this will include both Office applications and client agents. (See section **Error! Reference source not found. Error! Reference source not found.** below)
5. Endpoint Protection	• Configure, operate and maintain Microsoft Endpoint Protection on all Windows devices – including virtual clients and servers, ensuring that all devices receive emergency patches and definition updates on issue • Configure, operate and maintain device security through Microsoft 365 and Windows Defender Advanced Threat Protection • Manage anti-malware solutions for a small number of Linux devices. • Ensure that all operating systems are patched on at least a monthly cycle This includes responsibility for ensuring that both functional and security OS updates are successfully published to client devices. • Ensure that all non-emergency security patches are issued to devices on an agreed schedule and that devices are maintained at N-1 standard for functional patches and updates.
6. Virtual Desktops and Applications	• Configure, operate and maintain the Remote Desktop Server and Windows Virtual Desktop infrastructure in Azure to provide support for: ○ Thin client users in meat premises (RDS) ○ Third party support partner access to FSA internal systems (WVD) ○ Contingency use by FSA staff pending device swap-outs (WVD) ○ Secure access to internal applications and PSN services (WVD) ○ Service scaling and provision of new Host Pools ○ The FXLogix function

Service	Requirement
	• Configure and operate the publication of virtual applications within the above environment
7. Mobile Network Access	• Manage the provision of SIM cards including hotspots to end users of mobile devices, ensuring that all phones are issued with mobile network connectivity at setup. • Work in partnership with FSA's mobile network providers to: ○ Provide new mobile phone users with access to the network with best coverage in their area. ○ Resolve incidents and problems relating to mobile network connections
8. Branch Office Servers	• Take the technical lead in a project to decommission the branch office server infrastructure (comprising a single Hyper-V host and 3-4 virtual servers) in each of the five FSA offices and migrate residual services to the cloud-hosted environment • Manage and maintain the branch office server infrastructure pending decommission
9. Print Management	• Provide a joined-up Print Management service (preferably Software as a Service) for: ○ Shared printers in c 200 meat premises to provide printing both from RDS/WVD sessions and form users' mobile devices ○ A small number Home Users who have FSA issued secure printers

Transformation Requirements

Service	Requirement
1. Device Provision	• Ensure that provision and support of user endpoints is, on an ongoing basis, targeted towards a diverse, mobile and home-based workforce making increasingly less use of traditional office facilities for business activities • Develop systems and processes to provide a user service in which the provisioning of all equipment will provide the closest user

Service	Requirement
	experience to purchasing their own device (i.e.: plug it in, download the config, start using it). • The Endpoint Management provider should tailor the service to allow for an increased mix of FSA issued and user owned equipment, especially in the mobile device area.
2. Thin Client Migration	• Work with FSA and with Application Support partners to improve services to meat premises workers (this may include transitioning from the current shared thin client solution to individually issued mobile devices). • Provide technical, support and contractual architectures to enable an increased variety of mobile device types to meet the requirements of different operational task workers.
3. Virtual Desktops and Applications	• Work with FSA to enable, for example, WVD to be used as part of a potential BYOD option and to enable secure access to line of business applications, enabling the distinction between physical and virtual devices to become increasingly seamless to end users. • Work with FSA to transition: ○ The service to meat premises users from the current RDS setup to the WVD infrastructure ○ The WVD base model away from traditional “Gold Images”
4. Device Security	• Enable and support the increased use of biometrics (e.g. Windows Hello) for user authentication across all device types
5. Print Management	• The design for a Print Management solution should allow for the inclusion of office network printers at the end of the current Print Management contract in 2022. Precise numbers and locations are tbc pending confirmation of post-Covid 19 occupancy levels and estates strategy
6. Conferencing Equipment	• Dependent on post-Covid 19 occupancy levels and estates strategy: ○ Configure, operate and maintain Teams Rooms devices in FSA office meeting rooms

Service	Requirement
	○ Design layouts and equipment requirements for meeting and conference rooms following revised occupancy specification of room numbers and capacities. Advise and support the resultant FSA procurement of Teams Rooms devices. ○ Provision and maintain meeting room layout and equipment to provide effective protection against accidental damage or tampering
7. Technology Roadmap **(See FS430633_015 ODD IT Evergreen Technology Roadmap)**	• 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 8:01pm to 6:59am 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 **(See** FS430633_014 FSA IT	• The support partner shall adhere to the FSA User Access policy. Role based user access must be supported and integration with Azure AD	Must

Description	Purpose	Priority
Acceptable Use Policy Nov 2020 v3.2)		
Assistive Technology	• The support partner will be responsible of the full management of the assistive hardware and software	
GDPR	• The support partner must comply with their responsibilities under GDPR	Must
Service Management (**See** FS430633_006 FSA Acceptance Into Service Procedure, FS430633_007 FSA Change Management Procedure, FS430633_008 FSA Incident Management Procedure, FS430633_009 FSA Security Incident Procedure 2019, FS430633_010 FSA Problem Management Process, FS430633_011 FSA Knowledge Management Procedure, FS430633_012 FSA Service Asset & Configuration Mgt Procedures, FS430633_016 FSA Request Fulfilment, FS430633_017 Service Level Agreements, FS430633_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

Description	Purpose	Priority
Storage	• The Support Partner will be asked to provide capacity for a maximum number of working devices and maintain stock levels to meet FSA's service levels • The Support Partner will be asked to store devices for disposal. A minimum level of 50 devices will need to be stored before collection for disposal • Secure storage of FSA device • The Support Partner must ensure that relevant insurance is in place	Must
Courier Services	• The Support Partner will be responsible for shipping and collection of devices across the UK.	Must
Device Disposals	• FSA has an existing disposals supplier but may look to include this in Endpoint Management services over the life-time of the contract • If required FSA are happy for the supplier to utilise the FSA's existing disposals contract, but the Support Partner will be responsible for coordination and management of the disposals process.	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
Support Partner's End User Devices	• The support partner shall ensure that: ○ 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

Description	Purpose	Priority
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	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

Little Fish Qualification Envelope Responses

PROJECT INFORMATION

Project Code	Project Title	Project Reference
project_676	FS430633 - End Point Management	FS430633

ITT SETTINGS

ITT Code	ITT Title	ITT Description
itt_422	FS430633 - End Point Management	

Type of Supplier Access	Options for Viewing Responses	Ranking Level	Current Awarding Level
By Invitation Only	Sealed (parallel opening)	Overall	

Qualification Envelope	Technical Envelope	Commercial Envelope
Yes	Yes	Yes

Supplier Response Ranking	Commercial Envelope Strategy	ITT Status
No Ranking		Technical Evaluation

Estimated Value of Contract	Currency:	
	GBP	

QUALIFICATION RESPONSES EVALUATION DETAILS (*)

Report run from: Report Area, at: 25/03/2021 09:28

Number of Responses	1
Number of Questions	34

Supplier	LITTLE FISH (UK) LIMITED
Supplier Evaluation	Accepted
Acceptance or Rejection Notes	

Section Name	1.1 Service Qualification Questions

Note	**Note Details**
1.1.1 Service Qualification questions	If you answer No to any of the below Service qualification questions please do not respond to this Invitation to Tender.
Response	

Question	**Description**
1.1.2 1	Please confirm you have demonstrable experience of using Microsoft Autopilot and Endpoint Manager (aka Intune) to manage Windows and Mobile devices.
Response	
Yes	

Question	**Description**
1.1.3 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. Please confirm you accept this.
Response	
Yes	

Question	**Description**
1.1.4 3	Please confirm that you are structured and equipped to support end user devices in a Remote First organisation with limited use of FSA office space.
Response	
Yes	

Question	**Description**
1.1.5 4	Please confirm that you can provide secure storage at a registered premise for a maximum buffer stock of 180 devices.
Response	
Yes	

Question	**Description**
1.1.6 5	Please confirm you have experience working in a multi-Supplier model. For

Question	Description
1.1.6 5	example, dependant on other Suppliers while those Suppliers also have dependencies on you as our Support Partner.
Response	
Yes	

Question	Description
1.1.7 6	Accessibility - The supplier will ensure that all services and documentation meet accessibility standards (currently WCAG 2.1 AA) for their area of responsibility. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.8 7	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. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.9 8	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 8:01pm to 6: 59am Monday to Friday plus weekends and bank holidays. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.10 9	ITSM Toolset (ServiceNow) - The supplier will work within the FSA's ServiceNow instance with respect to all service management processes. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.11 10	ITSM Toolset (Snow) - The supplier will work with FSA's Snow instance for software asset management. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.12 11	Insurance - The Supplier must ensure that relevant insurance is in place to protect FSA Assets in their storage facility. The supplier is to acknowledge full liability once they are in receipt of any FSA devices. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.13 12	Shipping - The Supplier will provide and manage courier service for deployment and return for all end user devices. Please confirm you accept this.
Response	
Yes	

Question	Description
1.1.14 13	Resource - The supplier will provide a named Service Delivery Manager. Please confirm you accept this.
Response	
Yes	

Section Name	1.2 Security Qualification Questions

Note	Note Details
1.2.1 Security Qualification Questions	If you answer No to any of the below Security qualification questions please do not respond to this Invitation to Tender.
Response	

Question	Description
1.2.2 11	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. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.3 12	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 accept this.
Response	
Yes	

Question	Description
1.2.4 13	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 accept this.
Response	
Yes	

Question	Description
1.2.5 14	Identity, Authentication and Access Control - The supplier will provide an access control regime that ensures all users and administrators of the Supplier System/Service are uniquely identified and authenticated when accessing or administering the Services. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.6 15	Identity, Authentication and Access Control - The Supplier will apply the 'principle of least privilege' when setting access to the Supplier System/Service so that access is set for only parts of the Supplier System/service they and FSA users and other suppliers require. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.7 16	Event Logs and Protective Monitoring - The Supplier shall collect audit records which relate to security events that would support the analysis of potential and actual compromises. The Supplier will take a protective approach to reviewing these audit records. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.8 17	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 back ups) without the prior written consent of the FSA. The Supplier must also provide the locations within the EEA where data is stored. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.9 18	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. The supplier will deploy a tool to protect the service from malicious software. The supplier will monitor and mange the alerts and if malicious software is found the supplier will be responsible for managing the incident and removal in line with NCSC guidelines. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.10 19	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 will accept this.
Response	
Yes	

Question	Description
1.2.11 20	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 accept this.
Response	
Yes	

Question	Description
1.2.12 21	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 accept this.
Response	
Yes	

Question	Description
1.2.13 22	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 In particular principles 1 and 2. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.14 23	Endpoint Protection - The Supplier will ensure USB external interface protection is implemented which meets our user needs for allowed devices. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.15 24	Endpoint protection - The Supplier will implement app locker to protect against

Question	Description
1.2.15 24	unauthorised and malicious software. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.16 25	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 accept this.
Response	
Yes	

Question	Description
1.2.17 26	Certification - Please confirm you have Cyber Essentials PLUS.
Response	
Yes	

Question	Description
1.2.18 27	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
1.2.19 28	Incident and Breach Management - reporting - If the Supplier becomes aware of a Breach of Security covering FSA data (including a Personal data breach) the Supplier will inform the FSA at the earliest opportunity. Please confirm you accept this.
Response	
Yes	

Question	Description

1.2.20 29	Vulnerabilities and Patching - the Supplier shall deploy security patches for vulnerabilities in the service within: 3 days after the release for High vulnerabilities, 14 days after release for Medium and 30 days for low. Please confirm you accept this.
Response	
Yes	

Crown
Commercial
Service

Little Fish Operational Response

1.1 TENDER	1.2 FS430633 Endpoint Management

Section 1: Device Management – 30%

A Manage the provisioning of end user devices, including laptops, tablets, thin client devices and mobile phones, for issue to FSA staff. This will include receipt of devices from our hardware provider, storage of buffer stock and pre-enrolment ahead of dispatch to end users. Ensure that provision and support of user endpoints is, on an ongoing basis, targeted towards a diverse, remote and home-based workforce with no requirement to attend FSA offices for the issue of equipment or resolution of incidents and requests.

Q1 - Describe your experience of deploying Windows devices to a predominantly remote working organisation. Your answer should include a description of how you initially deployed the devices and how you support end users on an ongoing basis – 15%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]
Q2 - Describe your experience of deploying and supporting Android and IOS mobile devices for a predominantly remote working organisation. – 15%
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted] [redacted]
Q3 - Describe how you would take over the management of the thin client devices that are currently deployed to c 200 meat plants and how you will approach the deployment of equipment to new sites (c 2 per year) – 15%
[redacted] [redacted] [redacted] [redacted]

[redacted]

B Proactive management of the device provision to ensure all staff members devices needs are met without delay.

Q4 - How will you minimise the deployment time to end user for device requests? – 5%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted] [redacted]
Q5 - Describe how you will support users and in particular new staff members in understanding the use of the device and embedding this knowledge? –5%
[redacted] [redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C Store and issue a buffer stock of devices, delivered by FSA's hardware suppliers, and issue these direct to users' home or corporate addresses.

Q6 - Describe how and where you will store and issue a buffer stock of devices, delivered by FSA's hardware suppliers, and issue these direct to users' home or corporate addresses. – 15%

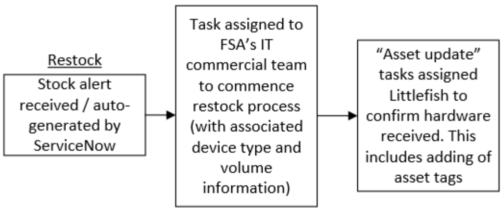
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]


Restock
Stock alert received / auto-generated by ServiceNow
Task assigned to FSA's IT commercial team to commence restock process (with associated device type and volume information)
"Asset update" tasks assigned Littlefish to confirm hardware received. This includes adding of asset tags

[redacted]

[redacted]

[redacted]

a. [redacted]

[redacted]

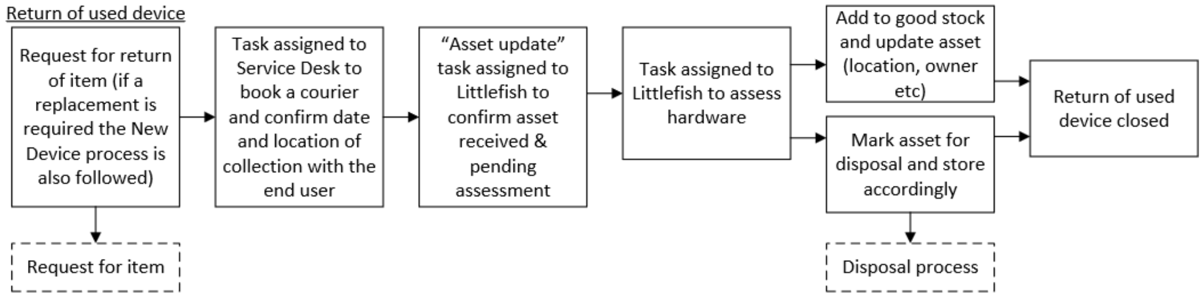
[redacted]

D Be responsible for the replacement and decommission of end user devices, including retrieval from plants, corporate offices and from users' home address and storage pending reissue or disposal.

Q7 - Describe how you will replace and decommission end user devices, including retrieval from plants, corporate offices and from users' home address. – 15%

[redacted]

[redacted]


Return of used device
Request for return of item (if a replacement is required the New Device process is also followed)
Request for item
Task assigned to Service Desk to book a courier and confirm date and location of collection with the end user
"Asset update" task assigned to Littlefish to confirm asset received & pending assessment
Task assigned to Littlefish to assess hardware
Add to good stock and update asset (location, owner etc)
Mark asset for disposal and store accordingly
Disposal process
Return of used device closed

[redacted]

[redacted]

Q8 - How will you identify, and agree with FSA a process of assessment to ascertain whether a device can be re-issued after repair or swap-out or whether it must be disposed of? – 15%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 2: Operational Asset Management – 10%

A Manage the lifecycle of assets for both hardware and software, ensuring appropriate asset control, management of the asset / CMDB records for assets in ServiceNow and SNOW, stock and licence management, allocation and distribution of assets through request fulfilment, Audit of asset records to ensure accuracy and compliance, license harvesting, control of unused assets and advising the FSA in the planning for replacement of End of Life Assets.

Q9 - Describe how you will manage the hardware and software asset lifecycles. – 50%

Your answer should outline how you will ensure appropriate asset control, management of the asset / CMDB records for assets in ServiceNow, stock and licence management, allocation and distribution of assets through request fulfilment, Audit of asset records, license harvesting, control of unused assets (e.g. no use recorded for 90 days) and advising the FSA in the planning for replacement of End of Life Assets

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B Proactively identify end of life and approaching end if life hardware, operating systems and client applications and work with FSA on the decommission of legacy.

Q10 - How will you proactively identify end of life and approaching end of life hardware, operating systems and client applications and support legacy decommission? – 50%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 3: Operating Systems – 10%

1.10	A Maintain and support client, mobile and server Operating Systems. This currently includes the following OS: Windows 10, Windows Server, Android, IOS, Red Hat, Ubuntu and CentOS Linux, Microsoft Hyper-V, Wyse Thin-OS, IGEL
1.11	Q11 - FSA has identified that operating system software should be supported as a collective service, without distinction between desktop, mobile and server OS.
1.12	Describe how you will operate, maintain and continually improve an environment that, while predominantly Windows 10, also includes Windows Server, Android, IOS, Red Hat, Ubuntu and CentOS Linux, Microsoft Hyper-V, Wyse Thin-OS, IGEL – 30%

1.13 Littlefish currently provide support for over 75,000 endpoints worldwide. These endpoints cover laptops, desktops, mobile devices (including tablets), thin clients, and servers. Whilst a number of components and operating systems are common across most managed services, our current core supported devices range across:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

1.14	B OS updates, including Windows 10 Service Channel Updates, will form part of the standard service. Ensure that Operating Systems, are maintained at N-1, are compliant with meet NCSC Baseline Security standards and that OS version updates are rolled out across devices on a schedule to meet this requirement.
1.15	Q12 - With particular reference to Windows 10 Channel Updates, how will you ensure that Operating systems are maintained at N-1 while minimising the disruption to end users resulting from the upgrade process. – 25%
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]	
1.16	C Ensure that individual Windows and Linux virtual server Operating Systems (in the Azure IaaS environment supported by FSA's Cloud Infrastructure Management partner) are maintained at N-1, are compliant with meet NCSC Baseline Security standards and that OS version updates are rolled out across devices on a schedule to meet this requirement.
1.17	Q13 - How will you ensure that individual Windows and Linux Server operating systems receive regular patches and anti-malware updates and meet the required levels of compliance with N-1 and NCSC standards? – 10%
[redacted]	

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]	
1.19	Q14 - How will you approach server operating system monitoring and ensure the appropriate pro-active action in response to errors and alerts? – 15%
[redacted] [redacted]	

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

1.20	D Pro-actively monitor all supported hardware and software for end of life and end of support. Advise FSA of, and initiate, appropriate remedial actions
1.21	Q15 - How will you pro-actively monitor all supported hardware and software for end of life and end of support and advise FSA of, and initiate, appropriate remedial actions? – 20%
1.22	

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 4: Device Management Tools – 15%

A Manage End User Devices using Microsoft Endpoint Management (aka Intune)

Q16 - Describe your experience of using Microsoft Intune and Autopilot for enterprise management of Windows devices – 20%

Your answer should describe how you will use the toolset to provision, and support end users in the configuration of, devices without a dependency on access to FSA offices.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Q17 - While an estate managed by Intune is FSA's objective, initially there will still be a substantial number of devices operated through traditional SCCM Gold Builds.

How will you manage the initial split estate to ensure consistency for end users while working with us to complete the transition to Intune? – 10%

[redacted]

[redacted]

[redacted]

[redacted]

B Configure, operate and maintain Device Configuration and Compliance policies, ensuring that devices are configured in line with NCSC guidelines and are managed centrally to ensure ongoing compliance. This includes the remote wipe and reset of compromised or missing devices
Q18 - Describe how you will deploy Endpoint Configuration and Compliance policies to a variety of devices, ensuring that the policy definitions meet NCSC security guidelines whole at the same time being responsive to user needs. How will you ensure that approved changes do not result in "policy bloat"? – 20%
[redacted] [redacted] [redacted] [redacted]

C Configure, operate and maintain Windows Autopilot, Android Enterprise and Apple Business Manager for device enrolment.
Q19 - Give an example of when you have supported Android Enterprise and Apple Business Manager for device enrolment – 20%
[redacted] [redacted] [redacted] [redacted] [redacted]
D Configure, operate and maintain the packaging and distribution of applications through distribution tools such as MS Company portal and FSA's Play, Apple and Microsoft Stores.
Q20 - Outline your approach to the packaging and distribution of applications through MS Company portal, Google Play, Apple and Microsoft Stores and how you will support application requests and user self-service – 10%

[redacted]

[redacted]

[redacted]

E Configure, operate and maintain device management tools for systems not covered by Microsoft Endpoint Manager (e.g. Dell Wyse tools for thin client management)

Q21 - Microsoft Endpoint Manager will be the primary device management tool, but other systems will be required, in particular Dell-Wyse management tools for thin-client devices. What experience do you have of supporting these? – 10%

[redacted]

[redacted]

[redacted]

F Maintain and keep updated a standard set of software for download and installation during device setup; this will include both Office applications and client agents. (See FSA430633_001 Endpoint Management Specification Document - 11.2 Published Applications)

Q22 - FSA wishes to avoid the traditional "gold build" approach to client configuration. Please describe how you will support this approach while continuing to ensure that client software is maintained - and issued - using the latest version at any given time – 10%

[redacted]

[redacted]

[redacted]

Section 5: Endpoint Protection – 10%

A Configure, operate and maintain Microsoft Endpoint Protection on all Windows devices – including virtual clients and servers - taking a risk based approach to the release of emergency patches and definition updates.

Q23 - Describe how Endpoint Protection will be deployed to the device and Virus/ Malware definitions maintained and kept up to date, ensuring that all devices receive emergency patches and definition updates. Please note that this includes virtual clients and servers – 20%

[redacted]

[redacted]

[redacted]

[redacted]

B Configure, operate and maintain device security through Microsoft 365 and Windows Defender Advanced Threat Protection

Q24 - Describe how you would configure, operate and maintain device security through Microsoft 365 and Windows Defender Advanced Threat Protection and Bitlocker disk encryption – 20%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C Manage anti-malware solutions for a small number of Linux devices.

Q25 - How will you provide anti-malware solutions to the same level for non-Microsoft operating systems, e.g. Linux servers – 20%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

D Ensure that all operating systems are patched on at least a monthly cycle This includes responsibility for ensuring that both functional and security OS updates are successfully published to client device and that emergency patches are distributed on release.

Q26 - Describe your approach to managing the patch status for all client devices and operating systems - including those which "self-update", those which require configuration of a patch deployment service, and those which require custom updating. – 20%

[redacted]

[redacted]

[redacted]

[redacted]

E Ensure that all non-security updates are issued to devices on an agreed schedule and that devices are maintained at N-1 standard for functional patches and updates.

Q27 - How will you ensure that, in addition to the regular patching schedule, client installed applications devices are maintained at N-1 standard for functional patches and updates? – 20%

[redacted]

[redacted]

Section 6: Virtual Desktops and Applications – 10%

A Configure, operate and maintain the Remote Desktop Server and Windows Virtual Desktop infrastructure in Azure to provide support for:
o Thin client users in Meat Plants (RDS)
o Third party support partner access to FSA internal systems (WVD)
o Contingency use by FSA staff pending device swap-outs (WVD)
o Secure access to internal applications and PSN services (WVD)
o Service scaling and provision of new Host Pools
o The FXLogix function

Q28 - Please give an example of when you have supported and or deployed Windows Virtual Desktops (WVD) and supported Windows Server Remote Desktop (RDS) for an

organisation. What lessons learned form that will you bring to supporting the service for FSA – 60%
[redacted] [redacted] [redacted] [redacted]

[redacted]

B Configure and operate the publication of virtual applications within the above environment

Q29 - What is your experience of publishing virtual applications using WVD and App-Attach? – 40%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 7: Mobile Network Access – 5%

A Manage the provision of SIM cards to end users of mobile devices, ensuring that all phones are issued with mobile network connectivity at setup.

Q30 - Outline how you will work with FSA's mobile network suppliers to ensure that new recipients of mobile devices are able to connect to the mobile network on receipt – 50%

[redacted]

[redacted]

[redacted]

[redacted]

B Work in partnership with FSA’s mobile network providers to:
o Provide new mobile phone users with access to the network with best coverage in their area.
o Resolve incidents and problems relating to mobile network connections

Q31 - Describe how you will work with mobile network providers to resolve issues where users need to be transferred to a network with better coverage – 50%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 8: Branch Office Servers – 5%

A Take the technical lead in a project to decommission the branch office server infrastructure (comprising a single Hyper-V host and 3-4 virtual servers) in each of the five FSA offices and migrate residual services to the cloud-hosted environment

Q32 - In line with our Estates Strategy, FSA is looking to remove the residual branch office servers from our 5 offices (comprising a single Hyper-V server hosting a Domain Controller, an SCCM Distribution Point and a local Print Server). Please describe how you would deliver the decommission without disruption to the services. – 70%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B Manage and maintain the branch office server infrastructure pending decommission

Q33 - How will you provide patching and break-fix support for these environments ahead of decommission? – 30%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 9: Print Management – 5%

A Provide a joined-up Print Management service (preferably Software as a Service) for:
1. Shared printers in c 200 meat plants to provide printing both from RDS/WVD sessions and form users' mobile devices
2. A small number Home Users who have FSA issued secure printers

Q34 - Describe how you will Provide a Print Management service, including swap-out and disposal, for shared printers in c 220 meat plants (with printing both from RDS/WVD sessions) and for Home Users who have FSA issued secure printers – 100%

Please note that the latter are used for printing Official-Sensitive material which is retained on device and must be disposed of in line with NCSC guidelines

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Little Fish Transformational Response

1.23 TENDER	1.24 FS430633 Endpoint Management

Section 1: Device Management and Provision – 20%

A Ensure that processes and tooling for Endpoint issue and management remain current and will support a Connectivity strategy based on a continual shift in dependency from core office networks and VPNs to direct internet access to services.

Q1 - How will you ensure that your processes and tooling for Endpoint issue and management remain current and will support a Connectivity strategy based on a continual shift in dependency from core office networks and VPNs to direct internet access to services? – 34%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B Develop systems and processes to provide a user service in which the provisioning of all equipment will provide the closest user experience to purchasing their own device (i.e.: plug it in, download the config, start using it). This will include ensuring that technical, support and contractual architectures will support multi-vendor hardware provision.

Q2 - As user expectations change, how will you develop systems and processes to provide a user service in which the provisioning of all equipment will provide the closest user experience to purchasing their own device.
Your answer should reference how you will enable and support multi-vendor hardware provision – 33%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C The Endpoint Management provider should tailor the service to allow for an increased mix of FSA issued and user owned equipment, in both the desktop and mobile areas

Q3 - FSA anticipates an increase in the use of users' own devices. How will you develop your service to allow greater flexibility in this respect without increasing the risk to information and device security? – 33%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 2: Mobile Device Scope – 15%
A Work with FSA and with Application Support partners to improve services to meat plant workers (this may include transitioning from the current shared thin client solution to individually issued mobile devices).
Q4 - It is anticipated that users based in meat plants will make increasingly more use of mobile applications and devices and reduce their requirement for shared thin-clients. Describe how you would propose to transition both your operational and service management approach in response to this – 50%
[redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

B Provide technical, support and contractual architectures to enable an increased variety of mobile device types to meet the requirements of different operational task workers

Q5 - How will you provide technical, support and contractual architectures to enable an increased variety of mobile device types to meet the requirements of different operational task workers over the lifetime of the contract? – 50%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 3: Virtual Desktops and Applications – 25%

1.32 A Work with FSA to enable, for example, WVD to be used as part of a potential BYOD option and to enable secure access to line of business applications, enabling the distinction between physical and virtual devices to become increasingly seamless to end users.

1.33 Q6 - FSA will make increased use of Windows Virtual Desktop (WVD) to provide access to both full Windows desktops and line of business applications. Describe how you will work with us to facilitate this and to provide seamless (from a user perspective) integration of physical and virtual devices. – 50%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

1.34	B Work with FSA to transition the service to meat plant users from the current RDS setup to the WVD infrastructure
1.35	Q7 - Describe how you will migrate access from Dell Wyse thin clients in Meat Plants from Windows Remote Desktop to WVD – 30%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]	
1.36	C Migrate the WVD base model away from traditional “Gold Images”
1.37	Q8 - How will you enable the migration of the WVD base model away from traditional “Gold Images” – 20%
[redacted]	
[redacted] [redacted] [redacted]	

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 4: Device Security– 10%

A Enable and support the increased use of biometrics (e.g. Windows Hello) for user authentication across all device types.

Q9 - How will you enable and support the increased use of biometrics (e.g. Windows Hello) for user authentication across all device types – 100%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 5: Print Management – 10%

A The design for a Print Management solution should allow for the inclusion of office network printers at the end of the current Print Management contract in 2022. Precise numbers and locations are tbc pending confirmation of post-COVID-19 occupancy levels and estates strategy.

Q10 - During the lifetime of the contract you will take over the management of network printers in 5 FSA offices. How will you ensure that the Print Management solution outlined in the Operational Requirements is scoped to enable this and how will manage the transition of both printer hardware and management software? – 100%
[redacted] [redacted] [redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 6: Conferencing Equipment – 10%
A Dependent on post-COVID-19 occupancy levels and estates strategy: **Configure, operate and maintain Teams Rooms devices in FSA office meeting rooms** **Design layouts and equipment requirements for meeting and conference rooms following revised occupancy specification of room numbers and capacities. Advise and support the resultant FSA procurement of Teams Rooms devices.** **Provision and maintain meeting room layout and equipment to provide effective protection against accidental damage or tampering**

Q11 - Please describe how you will implement and support Teams Rooms conferencing equipment in FSA Offices. In particular, how will you approach designing meeting room layouts to minimise the risk of damage to both devices themselves and their connectivity? – 100%
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

[redacted]

Section 7: Technology Roadmap – 10%

A Whilst this document specifies FSA's current technology and services, the supplier will be required to support the principle of the FSA IT's Evergreen Strategy to continually update, review and where appropriate adopt and benefit from new and emerging technology.

Q12 - Describe how you will regularly identify and showcase new technology relevant to the FSA's requirements and strategic direction – 15%

[redacted]

[redacted]

[redacted]

[redacted] [redacted]
Q13 - Describe how you will upskill and support the FSA as it upgrades and replaces existing services and adopts new technology – 10%
[redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

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

Q14 - Describe your approach to project delivery and how you will provide technical leadership to cross-supplier project teams – 25%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C Work with other suppliers to continually improve the technical infrastructure across all Service Groups.

Q15 - 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. – 25%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

Q16 - Describe your roadmap for delivery of service improvements in Endpoint technologies and service delivery over the next 12-24 months, including how new services will be made available to the FSA. – 25%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Crown
Commercial
Service

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Little Fish Service Response

1.39 TENDER	1.40 FS430633 Endpoint Management

Section 1: Service Management – 50%

A Service Improvement - Improve customer experience by adopting a 'shift left' approach, transferring knowledge to service desk to enable first line fix wherever possible

Q1 - Describe how you will identify resolutions that meet this criteria, and how you will continuously ensure these are transferred to enable first line fix – 5%

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B 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.

Q2 - 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 – 5%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

C 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.
Q3 - Describe your own processes for the acceptance of new services, and how these ensure you are able to provide appropriate support – 5%
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

Q4 - Describe your approach to change management and what actions you take to minimise the risks associated with changes – 5%

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

E Design Documentation - The supplier will provide high- and low-level design documents for all services and solutions, using templates agreed with FSA. 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.
Q5 - Describe your approach to design documentation and how you ensure that documents are accurate and up-to-date – 5%
[redacted] [redacted] [redacted] [redacted]
F Incident management - The supplier shall work to the FSA incident management process, and for their areas of responsibility contribute to the logging / categorisation, monitoring, escalation, evaluation and resolution of incidents within agreed timescales
Q6 - Describe your approach to incident and major incident management, and how you would identify and resolve incidents for your areas of responsibility – 10%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted] [redacted] [redacted]
G Security Incident Management - The Supplier will comply with the FSA security incident management policy (included in ITT supporting documents). All security incidents will be prioritised as a P2 or above.
Q7 – Please confirm you will agree to this - Yes/No response – 5%
Yes
H Knowledge management - 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 ensure the knowledge base is up-to-date and accurate for the services they support.
Q8 - Describe your approach to knowledge management and how you ensure that documents are accurate and up-to-date – 10%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

I 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 (EUD Compliance metrics, Malware Incidents and Resolution, Patching Compliance), 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. The supplier must produce a security compliance report on a quarterly basis in a format that can be shared and understood at board level for our Audit and Risk Committee. The monthly reports will show trend information and analysis for the last 12 months to demonstrate ongoing compliance.

Q9 - Explain your approach to a monthly performance reports and how you would highlight issues or areas of concern – 3%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

J Problem management - The supplier shall work to the FSA problem management process, and contribute to the identification, categorisation, prioritisation, diagnosis, resolution and evaluation / closure of problem management.

Q10 - Describe your approach to problem management and how you would contribute to identification and resolution of problems – 3%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

K Request management – The supplier shall work to the FSA request management process, and for their areas of responsibility contribute to the fulfilment, execution, monitoring, escalation and evaluation / closure of service requests.

Q11 – Provide examples of request management processes you have provided and how you ensure these are monitored and managed to achieve customer satisfaction – 15%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

L 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.

Q12 – Describe your approach to configuration management and how you would contribute to identification and updates of configuration items and dependencies – 15%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

M 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.
Q13 – Describe your approach to the analysis of customer satisfaction feedback, and how you would use these findings to improve service quality – 5%
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

[redacted]

N Business Continuity

Q14 - 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.

Please confirm that you agree to this – Yes/No Response – 0.5%

Yes

Q15 - The supplier will provide up to date Business Continuity plans for their organisation on an annual basis.

Please confirm that you agree to this – Yes/No Response – 0.5%

Yes

Q16 - 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 Endpoint Management services including provision of kit in a pandemic lockdown scenario – 3%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

Q17 – Explain how you will manage, monitor and achieve the expected performance criteria specified in the FSA SLA document – 5%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 2: Storage 2%

A Stock Management - The Supplier will provide capacity for a maximum number of working devices and maintain stock to meet FSA's service levels.

Q18 - Explain how you will manage stock to maintain the FSA's service levels for the provision of new and replacement kit – 25%

[redacted]

[redacted]

[redacted]

[redacted] [redacted]
B Physical Security
Q17 – The Supplier will provide suitable secure storage facilities taking account of the CPNI guidance for buildings https://www.cpni.gov.uk/building. Please confirm that you agree to this – Yes/No Response – 25%
Yes
Q19 - The Supplier will ensure that there is an appropriate visitors policy at the office where FSA assets are stored to prevent visitors being able to access to the assets. Please confirm that you agree to this – Yes/No Response – 25%
Yes
Q20 - The Supplier will apply a layered security approach to access to the office where FSA assets are stored using (e.g. locks and access control system) to mitigate the risk of intruders gaining access to the office where FSA assets are stored. Please confirm that you agree to this – Yes/No Response – 25%
Yes
Section 3: Courier Services – 2%
A Shipping - The Supplier will be responsible for shipping and collection of FSA IT equipment across the UK. If required FSA is happy for this service to be subcontracted, but the Supplier will be responsible for the full management of that relationship. This is expected to be a charge back service based on actuals.

Crown
Commercial
Service

Q21 - Explain how your organisation will operate such a service – 80%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted] [redacted] [redacted]
Q22 - The supplier will ensure that appropriate tracking information is provided, including notifications of dispatch and delivery dates to the recipient of kit and real time updates on dispatch and confirmed delivery in the Service Now request ticket. Please confirm that you agree to this – Yes/No Response – 20%
Yes
Section 4: Device Disposals – 1%
A Disposals - FSA has an existing incumbent disposal supplier, however may seek to include the disposal service into Endpoint Management contract at a later date.
Q23 - Explain your device disposals service (is it safe, secure, environmentally friendly?) and whether or not you offer re-marketing to offset costs on revenue made from this process. How would you guarantee smooth transition from the incumbent supplier to your disposal offering? – 100%
[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 5: Continuous Service Improvement – 10%

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.

Q24 - Explain how you will see to achieve this requirement and provide examples which have resulted in quality improvements or monetary savings – 50%

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

B Innovation - A core principle of for FSA is to ensure that suppliers continuously innovate and will not be confined by the contract to do so. It is hugely important that services are able to grow are technology innovates.

Q25 - Describe how you would achieve this and how you would engage FSA – 50%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 6: Ways of Working – 7%

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.

Q26 - Describe your experience of working with a range of different suppliers and how you are able to integrate successfully with them – 20%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Q27 - Describe your approach to complex or major incident management in a disaggregated service delivery model – 20%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

Q28 - Describe your approach to system testing for any services that you use and / or support – 15%

[redacted]

[redacted]

Crown
Commercial
Service

[redacted] [redacted] [redacted]
C Training - The supplier shall ensure that appropriate role-based training is conducted for FSA IT staff, resolver groups, other suppliers and end users where appropriate.
Q29 - Describe your experience of providing training to both IT staff and end-users – 10%
[redacted] [redacted] [redacted] [redacted]
D ITIL Principles - ITIL principles must be followed

Q30 - Describe how you ensure your staff have an appropriate understanding of ITIL principles – 1%

[redacted]

[redacted]

[redacted]

[redacted]

Q31 - Describe how you will ensure your staff members adopt and understand FSA's policies and procedures – 14%

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

E 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.

Q32 - Explain how you plan to resource this service offering, key personnel and escalation routes – 10%

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

F 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.

Q33 - Describe how you will ensure the services you provide are compatible with existing FSA's services – 10%

[redacted]

[redacted]

[redacted]

[redacted].

Section 7: Project Management – 1%

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

Q34 – Please confirm that you agree to this - Yes/No response – 50%

Yes

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

Q35 – Please confirm that you are able to provide this - Yes/No response – 50%

Yes

Section 8: 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.

Q36 – 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

Q37 - 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

Q38 – 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 9: Security – Identity, Authentication and Access Control – 5%

A Identity, Authentication and Access Control:

Q39 – The Supplier will provide reports/data on the records of access to the System/Service to the FSA on request.

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

Yes

Q40 – The Supplier will comply with the FSA access policy for access to FSA Systems/Services.

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

Yes

Q41 - The Supplier will ensure the service complies with the FSA principle to use Multi- Factor Authentication.

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

Yes

Q42 - The Supplier will be able to implement configurable role-based access to the Supplier System Service or FSA System/Service.

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

Yes

Section 10: Security - Event Logs and Protective Monitoring – 5%

A Event Logs and Protective Monitoring: The Supplier shall collect audit records which relate to security events that would support the analysis of potential and actual compromises. The Supplier will take a protective approach to reviewing these audit records.

Q43 - In order to facilitate effective monitoring such Supplier audit records will (as a minimum) include regular reports and alerts setting out details of access by users to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of FSA Data.

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

Yes

Q44 - The Supplier will produce monthly reports which document the compliance of the service and work together with the FSA at the inception of the contract to establish any additional audit and monitoring requirements.

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

Yes

Q45 - 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.

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

[redacted]

[redacted]

Q46 - The retention periods for audit records and event logs will be agreed with the FSA and documented.

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

Yes

Section 11: Security - Vulnerabilities and Patching – 5%

A Vulnerabilities and Patching: The Supplier shall deploy security patches for vulnerabilities in the service within: 3 days after the release for High vulnerabilities, 14 days after release for Medium and 30 days for low.

Q47 - The FSA and the Supplier acknowledge that from time to time vulnerabilities in the Supplier System/Service will be discovered which unless mitigated will present an unacceptable risk to the FSA Data. The Supplier will supply a copy of their patching strategy/policy and assessment process to FSA on request.

Pease confirm you agree to this - Yes/No response – 10%

Yes

Q48 - The timescales for applying patches to vulnerabilities shall be extended if the FSA agrees a different maximum period after a case-by-case consultation with the Supplier which could be; if the Supplier can demonstrate that a vulnerability is not exploitable within the context of the Services Pease confirm you agree to this - Yes/No response – 15%
Yes
Q49 - The timescales for applying patches to vulnerabilities shall be extended if the FSA agrees a different maximum period after a case-by-case consultation with the Supplier which could be; If the he application of a 'Medium' or 'High' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension. Pease confirm you agree to this - Yes/No response – 15%
Yes
Q50 - The Supplier will provide documented evidence to demonstrate the provisions for major version upgrades of the Supplier System or FSA System the Supplier is responsible for to ensure it is always in mainstream support and complies with FSA patching policy of n-1 unless otherwise agreed by the FSA in writing. Pease confirm you agree to this - Yes/No response – 10%
Yes
Q51 - The Supplier will regularly test for the presence of known vulnerabilities and common configuration errors. Pease confirm you agree to this - Yes/No response – 10%
[redacted] [redacted]

[redacted]

B The suppliers shall adhere to the FSA patching policy, ensuring that all software and firmware is patched to a minimum of N-1 and there is a regular patching schedule in place with agreed maintenance windows

Q52 - Describe your approach to patch management and how you might implement this to ensure patching requirements are met in accordance with FSA policy – 40%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 12: 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

Q53 - Pease confirm - Yes/No response – 100%

Yes

Section 13: Security Testing: IT Health Check – 1%

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

Q54 - Pease confirm you agree to this - Yes/No response – 100%

Yes

Section 14: Security – Assurance – 4%

A Assurance

Q55 - 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 – 25%
Yes
Q56 - 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 – 25%
Q57 - 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 – 25%
Q58 - 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 – 25%
Section 15: Security – Compliance Audits – 4%
A Compliance Audits
Q59 - 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

Crown Commercial Service

Little Fish Commercial Response

1.50 TENDER	1.51 FS430633 Endpoint Management

Section 1: Transition Cost – 10%

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

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]

	[redacted]
	[redacted]
	[redacted]
[redacted]	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]
[redacted]	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]

[redacted]

Section 2: Initial Fixed Monthly Costs – 70%

A To ensure that FSA have a full understanding of potential costs, this supplier must provide an initial fixed month cost.

Q2 - Using the metrics supplied, you are required to provide your initial monthly fixed price costs - 100%

[redacted]

Section 3: Flexible Charging – Decrease – 5%

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

1.60 Q3 - Explain and demonstrate how you would adjust the fixed monthly cost if the current estate metrics were reduced by 10%, 50% and 90%. Please note those charges which are fixed for the entirety for the contract. Can you provide a breakdown of those decreased charges? – 100%

1.61

[redacted]

[redacted]

Section 4: Flexible Charging – Increase – 5%

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

Q4 - Explain and demonstrate how you would adjust the fixed monthly cost if the current estate metrics were increased by 10%, 50% and 90%. Please note those charges which are fixed for the entirety for the contract. Can you provide a breakdown of those increased charges – 100%

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 5: Change Management – 2%

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.

Q5 - Can you explain how your organisation will be able to meet this requirement and if there are any thresholds to such a change. Include how instigating a change to contract will affect charges including the use of minimum annual charges or price caps. – 100%

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 6: Project Activity – 6%

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

Q6 - Can you supply your definition and any threshold between Business As Usual and project activity – 100%

[redacted]

[redacted] [redacted] [redacted] [redacted] [redacted]
Section 7: Early Termination – 2%
A FSA are keen to understand the suppliers postion on early termination costs.
Q7 - Can you supply details of what early termination costs you would expect FSA to pay and the level of any caps on any amounts payable to the supplier – 100%
[redacted]
Section 8: Rate Card - 0% (this is not part of the scored evaluation but for the FSA's reference
A Rate Card
Q8 – Please provide your project rate card, to help the FSA understand potential project costs over contract lifetime – 0%

Please see our Rate Card attached to the tender submission as "LF-Professional Services Rate Card v1.0"

Littlefish - Professional Services Rate Card

Standard Consultancy Rate Card

Resource Type	Day Rate
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Littlefish Resource Definitions

Follow – Entry level IT capability (supervised activities)
Assist – Desktop and Deskside delivery capability
Apply – Server, Network and Cloud Implementation capability
Enable – Server, Network and Cloud Configuration capability
Ensure/Advise – Server, Network and Cloud Design capability and Lead Project Engineer; Project Management Capability
Initiate/Influence – Solution Architect
Set Strategy / Inspire – Enterprise Architect or CTO capability

Standards for Consultancy and Cyber Security Day Rates

[redacted]

A Full Day is considered to be 09:00 to 17:30 (with 30 minute lunch). A Half Day equates to up to 4 hours of activity. Project activity delivered outside of 09:00 to 17:30 Monday to Friday will be charged at the variable Out of Hours, Weekend and Public Holiday Rates defined above.

Crown
Commercial
Service

Little Fish Clarification Questions and Responses

Requests for clarification and additional information

Question 1: In the Endpoint Service response template, Section 14: Assurance questions 56 – 58 have been not been responded to (yes/no answers).

Q56 - The Supplier will work with the FSA to complete a Personal Data Processing Statement as part of the contract.

Q57 - The Supplier will work with the FSA to mitigate any risks assigned to them in the Privacy Impact Assessment if applicable.

Q58 - 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.

Please can you confirm whether you agreed to these requirements or not (yes/no response)?

Response:

Apologies – busy with the narrative questions this slipped though.

For completeness:-

Q56 - The Supplier will work with the FSA to complete a Personal Data Processing Statement as part of the contract.

Yes

Q57 - The Supplier will work with the FSA to mitigate any risks assigned to them in the Privacy Impact Assessment if applicable.

Yes

Q58 - 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.

Yes

Crown
Commercial
Service

Requests for clarification and additional information

Question 1: Initial Fixed Monthly Costs – Commercial Template. Assumptions tab, no 8 and 10. Both rows refer to 'Service Requirements - Section 3: Courier Services states "This is expected to be a charge back service based on actuals". The assumption in no 8 goes on to suggest that there will be additional costs for 'repairs'. I understand that the courier costs are unknowns and chargeable, but actual repair should be included in the monthly fixed costs. Can you clarify please that your Assumptions are referring to an unknown cost for 'courier charges' only and that repairs are included in the fixed monthly fee?

Response:

If a device needs to be physically repaired and it is outside warranty, Littlefish will manage and assist the FSA in obtaining a quote and providing a recommendation whether to proceed or dispose of the device. This is included in the monthly fee and assumes that a high proportion of devices in FSA's estate that are subject to support by the Endpoint Management service have active warranty and appropriate repair contracts in place. Providing user home visits, for example.

We would work with the FSA for guidance on where the line between economical to repair and not economical to repair sits for each devices type. Our existing knowledge of FSA's estate together with detail gathered across our wider Customer base would act as intelligent input in to this conversation

The monthly fee does not include a 'Repair Service' – Littlefish will manage devices against their existing warranty process. If a device is not under warranty (confirmed at point of contact by the Service Desk) it enters triage with one of two paths:-

1) The Service Desk (and Endpoint Management engineer if required) confirm it is not economical to repair the device given predefined guidance from the FSA and evidence gathered from the user. It is disposed of and a priority new device process is triggered
2) The Service Desk (and Endpoint Management engineer if required) confirm it might be economical to repair given predefined guidance from the FSA and evidence gathered from the user so they obtain a quote from the manufacturer (Lenovo for example). FSA either approve the quote* and the work is scheduled or the device is disposed of and a priority new device process is triggered.

* This process carefully considers the user without a working device. In that instance quick provision is a priority. Together, we may consider using a WVD workspace to keep the user up and running in the interim. This is all part of the Incident process that triggered the 'Repair?' question.

Crown
Commercial
Service

Post Tender Clarifications

PROJECT REFERENCE : FS430633
PROJECT TITLE : Endpoint Management

Date : 02 August 2021

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

1. The Tender is revised as follows:

Clarification/Revision 1: The attached template (FS430633 - LF - Initial Fixed Monthly Costs commercial Template_revised_18052021) contains the following revisions:

1. **Removal of the fixed monthly costs for Infrastructure Analyst (Windows)**
2. **Removal of the fixed monthly costs for Infrastructure Analyst (Linux)**
3. **Reduction in Cyber Security Analyst resource – from 8.7 to 4.8 days**
4. **Removal of the fixed monthly costs for Travel and Subsistence (Service Manager)**
5. **Reduction of 5% applied to total cost.**

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:

For the Authority		**For the Contractor**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Title:	[redacted]	Title:	[redacted]
Date:	[redacted]	Date:	[redacted]

ANNEX B – Work Package Template

FS430633
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: ● *[**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 FS430633 – Endpoint Management.

Signed on behalf of the FSA

Name:

Signature: --

Position:

Date:

Signed on behalf of the Supplier

Name:

Signature: --

Position:

Date: