



Technology Services 2 Agreement RM3804
Framework Schedule 4 - Annex 1

Order Form

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

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

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

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

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

Section A General information

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

Customer details

Customer organisation name

Food Standards Agency

Billing address

Your organisation's billing address - please ensure you include a postcode

Foss House, Kingspool, Peasholme Green, York, YO1 7PR

Customer representative name

The name of your point of contact for this Order

[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
Methods Business and Digital Technology Limited

Supplier address

Supplier's registered address
Saffron House, 6-10 Kirby Street, London EC1N 8TS

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
[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

N/A

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 | <input type="checkbox"/> |
| 2. TRANSITION & TRANSFORMATION | <input type="checkbox"/> |
| 3. OPERATIONAL SERVICES | |
| a: End User Services | <input type="checkbox"/> |
| b: Operational Management | <input checked="" type="checkbox"/> |
| c: Technical Management | <input type="checkbox"/> |
| d: Application and Data Management | <input type="checkbox"/> |
| 4. PROGRAMMES & LARGE PROJECTS | |
| a. OFFICIAL | <input type="checkbox"/> |
| a. SECRET (& above) | <input type="checkbox"/> |

Customer project reference

Please provide the customer project reference number.

FS430634

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

01/09/2021



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

24 Months

Call Off Extension Period (Optional) Months

12 Months (1 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

No Additional Standards Applicable

Customer's ICT and Security Policy

Please see Supporting documents:

FS430634_018 FSA Patching Policy Sept 2019 1.1

FS430634_014 FSA IT Acceptable Use Policy Nov 2020 v3.2

FS430634_013 FSA Supplier Access Policy August 2019 v1

FS430634_009 FSA Security Incident Procedure 2019

FS430634_006 FSA Acceptance Into Service Procedure

FS430634_007 FSA Change Management Procedure

FS430634_008 FSA Incident Management Procedure

FS430634_010 FSA Problem Management Process

FS430634_011 FSA Knowledge Management Procedure

FS430634_012 FSA Service Asset & Configuration Mgt Procedures

FS430634_016 FSA Request Fulfilment

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, the Suppliers responses to the ITT and any post tender Clarifications. 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.

The contract includes a full copy of the ITT response forms submitted by Methods and CoreAzure (including Operational, Service, Transformational and Commercial requirements). Collectively they form a useful record of how we have proposed to address the ITT requirements set out in the Business Requirements Section of the FSA Cloud Service Management Requirements Specification document version 2 (Reference: FS430634_001).

It should be noted however, that there are questions included within the ITT that do not relate to baseline contractual requirements and, to be properly fulfilled by the supplier, may either need to be resourced from the project allocation (or subject to change control), or to be completed have dependencies that are beyond the control of supplier. As such, not all of the statements covering service descriptions and commitments contained within the ITT response reflect a contractual commitment by the supplier. All statements regarding Methods and CoreAzure's capabilities within the ITT are an accurate reflection regardless of baseline or extended scope and/or project dependencies. Methods and CoreAzure's commercial response to Section 6 contains details of the baseline and capped services that are within scope of this agreement.

Location/Site(s) for provision of the Services

This service will be delivered remotely by the Supplier, with the occasional requirement to visit FSA Offices/Sites.

Additional Clauses (see Annex 3 of Framework Schedule 4)

This Annex can be found on the RM3804 CCS webpage. The document is titled RM3804 Alternative and additional t&c's v4.

Those Additional Clauses selected below shall be incorporated into this Call Off Contract

Applicable Call Off Contract Terms

Optional Clauses

Can be selected to apply to any Order

Additional Clauses and Schedules

Tick any applicable boxes below

Tick any applicable boxes below

A: SERVICES – Mandatory

The following clauses will automatically apply where Lot 3 services are provided (this includes Lot 4a & 4b where Lot 3 services are included).



A3: Staff Transfer

C: Call Off Guarantee



D: Relevant Convictions



E: Security Requirements





A4: Exit Management

A: PROJECTS - Optional

A1: Testing

☐

A2: Key Personnel

☒

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

☐

B: SERVICES - Optional

Only applies to Lots 3 and 4a and 4b

B1: Business Continuity and Disaster Recovery

☒

H: MOD Additional Clauses

☐

B2: Continuous Improvement & Benchmarking

☒

Alternative Clauses

B3: Supplier Equipment

☐

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

B4: Maintenance of the ICT Environment

☒

Tick any applicable boxes below

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

☐

Scots Law
Or

☐

B6: Indexation

☐

Northern Ireland Law

☐

B7: Additional Performance Monitoring Requirements

☐

Non-Crown Bodies

☐

Non-FOIA Public Bodies

☐

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

Not Applicable

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

Supplier Software

Not Applicable

Third Party Software

Not applicable

Customer Property (see Call Off Clause 21)


Items licensed by the Customer to the Supplier (including any Customer Software, Customer Assets, Customer System, Customer Background IPR and Customer Data)




List below if applicable
ServiceNow Licenses.


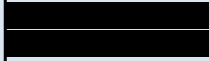
Any Devices Shared with the supplier to enable them to carry out aspects of the contract.

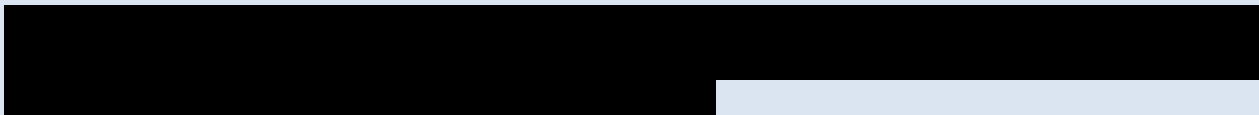
Call Off Contract Charges and Payment Profile (see Call Off Schedule 2)

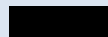
	
	

	
--	--

Undisputed Sums Limit (£)

Insert right (see Call Off Clause 31.1.1)



Delay Period Limit (calendar days)

Insert right (see Call Off Clause 5.4.1(b)(ii))

NA

Estimated Year 1 Call Off Contract Charges (£)

For Call Off Contract Periods of over 12 Months

	
--	--

Enhanced Insurance Cover

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

No Enhanced Insurance Cover required.



Transparency Reports (see Call Off Schedule 6)

If required by the Customer populate the table below to describe the detail (titles are suggested examples)

To be agreed between FSA and Methods during 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 FSA and Methods 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 and Methods attached to the Supplier's Catalogue Service Offer.

To be agreed between FSA and Methods during On-boarding of the service.

BCDR (see Call Off Schedule B1)

This can be found on the CCS RM3804 webpage. The document is titled RM3804 Alternative and additional t&c's v4.

Time frame for delivery of a BCDR Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days)

Where applicable insert right

45 days

Disaster Period (calendar days)

Services with availability SLAs for 24/7/365 = 1 working day

All other services = 2 working days.

GDPR (see Call Off Clause 23.6)

Please see Schedule 7 appended to this order form.

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.

Not Applicable

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 Responsibilities

List below or append as a clearly marked document



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)

Not Applicable

Appointment as Agent (see Call Off Clause 19.5.4)

Insert details below or append as a clearly marked document

Not Applicable

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

Introduction

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

- Core or 'working' hours 7:00am to 8:00pm Monday to Friday
- Non-core 8:00pm to 7:00am Monday to Friday plus weekends and bank holidays

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

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 unit experiencing significant	1 hour from assignment of issue	8 hours for critical services, 8 working	No more than 1 failure



	reduction in system performance.		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
Ensure changes are raised and submitted for any requests raised (except where agreed exceptions)	5 working days	100%

AD and Application 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.

Note: FSA's Patching policy is separate to these SLA, please refer to FS430634_018 FSA Patching Policy Sept 2019 1.1

Description	Target to be achieved in month
Hosted/SaaS/Configured server applications on the FSA estate are maintained at N-1 (except where agreed exceptions)	100% implementation for security patches / minor versions Deployment plan within 1 month for major versions
Windows AD Function Level are maintained at N-1 standard	100% implementation for security patches / minor versions



Deployment plan
within 1 month for
major versions

Additional KPIs

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

- Performance management of the FSA's Microsoft 365 tenants – Reporting of health and quality, compliance, usage and security.
- RCA within 3 working days for P1 and P2 incidents.
- Report on failed changes or changes causing issues with reasons.

Notes

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

Additional Performance Monitoring Requirements

Technical Board (see paragraph 2 of Call Off Schedule B7).

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 Methods 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	<p>There is no foreseen requirement of processing personal data under this contract, however the supplier will have access to personal data captured in ServiceNow, Active Directory and Microsoft 365 Admin Center.</p> <p>As this contract is for the support of Cloud Service Management it may be that the supplier is required to investigate certain incidents that include personal data.</p>
Duration of the processing	<p>Processing will take place over the duration of the contract. This is due to expire on the 31/08/2023 with an opportunity to extend by another 1 year (+1).</p>
Nature and purposes of the processing	<p>Microsoft 365: Name and FSA e-mail address are captured and stored in the Microsoft licensing admin portal for FSA. It is used to track the number of Microsoft licenses purchased and who they are assigned to in FSA.</p> <p>Service Now: Personal and staff data is captured and stored in the FSA's ServiceNow for the purpose of facilitating IT support at the FSA. It is used to log and track problems / incidents, as well as requests for staff equipment and specialist software.</p> <p>Active Directory: Staff data is stored in AD and is used primarily to authenticate users and endpoints in a windows domain.</p> <p>The supplier will not be required to contact the end users directly as this is managed by the FSA's Service Desk supplier.</p> <p>Data is stored in the FSA's ServiceNow, M365 and AD instances and no processing of personal data will take place outside of this, meaning there is no</p>



	<p>destruction of data required after this contract has expired.</p> <p>The supplier will be required to operate projects on behalf of the Agency. Should personal data be accessed it will be done so via FSA's infrastructure.</p>
Type of Personal Data	<p>Name, home address, personal phone number</p> <p>Staff data includes Name, Job Title, Department, staff Number, Grade, Work email and phone number, work location, Company and Manager.</p>
Categories of Data Subject	<p>Staff, contractors and suppliers.</p>
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	<p>Data will not be retained by the supplier.</p> <p>Personal data held by the supplier outside of the FSA infrastructure is required to be destroyed upon project completion.</p>

Annex A – Specification of Requirements and Methods ITT Response.

1 Statement of Requirements Purpose

The purpose of this document is to detail the business requirements for the provision of [Title], the operation and continual improvement of the interface between the technology infrastructure and business applications.

Cloud Service Management (CSM) focusses on maintaining application and data spaces and containers, specifically Microsoft 365. Its primary focus is on enabling FSA to make the best use of its Microsoft cloud service offerings, facilitate and provide platform support for application migrations from server-based Infrastructure as a Service (IaaS) to Platform and Software as a Service solutions (PaaS and SaaS).

The CSM supplier will work closely with the Cloud Infrastructure and Endpoint Management suppliers and with the FSA's own Openness Digital and Data (ODD) teams - including IT, Digital, Security and Data - and their development partners to ensure that line of business applications and services integrate into the overall IT architecture and that there is a joined-up, service-based support across diverse services.

The CSM supplier will provide technical support for our Microsoft 365 environment, including Exchange, SharePoint Online Services and Microsoft Teams, and will work alongside the FSA teams to provide new functionality and services to FSA end users in line with the Industry Roadmaps. This will include development and adoption of cloud services both within the Microsoft Azure and 365 tenancies and with other providers.

Microsoft 365 support includes support and maintenance for the FSA's Active Directory infrastructure and leading the transformation from an on-premise driven hybrid environment to Azure AD first.

The FSA has transformed our ways of working to become a primarily home and multi-site location organisation. Whilst Covid-19 has accelerated this, our expectation is this progression will continue with fewer staff using office space and on a more infrequent basis.

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

2 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, 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. 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. 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** FSA30634_015 ODD IT Evergreen Technology Roadmap]. This 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.

2.1 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>.

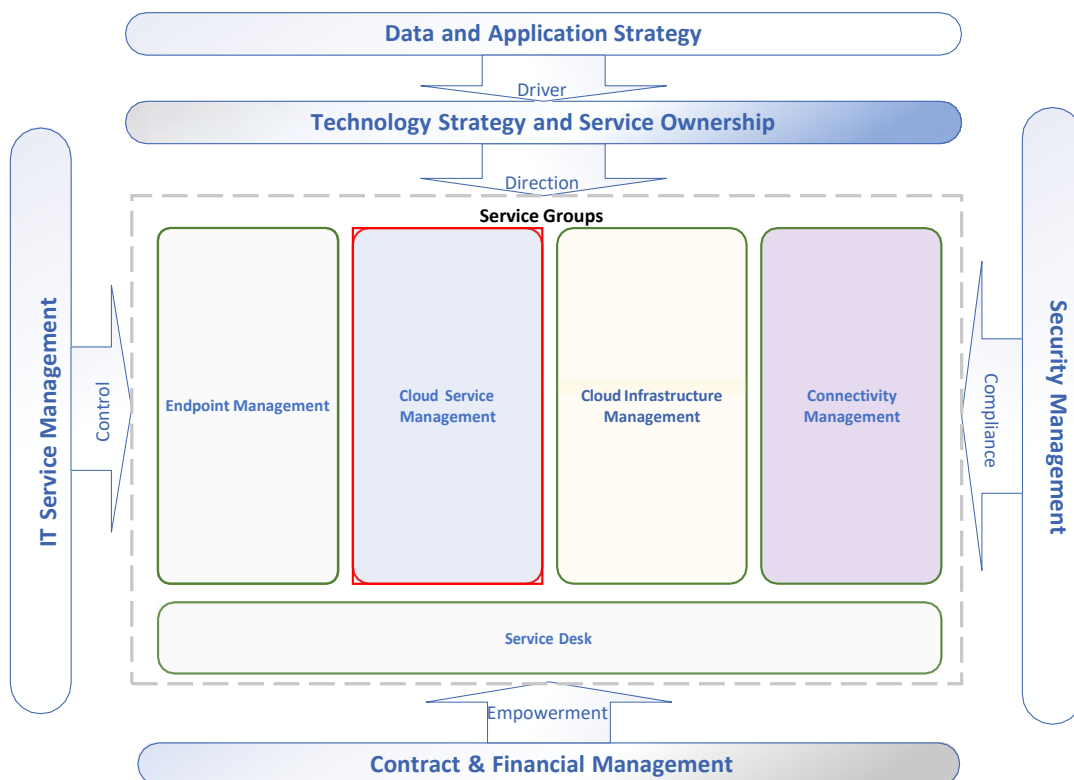
3 Commercial Approach

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

As part of this tender process FSA will not publish finances relating to existing actuals of incumbent suppliers 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.

4 General Specification

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





Endpoint Management (Tender Closed)	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 Management (This Tender)	What do we use it to do? The primary focus is enabling FSA to make the best use of cloud service offerings and facilitate and implement application migration from server based IaaS to Platform and Software services, as well as the ongoing management and improvement of our Microsoft 365 environment
Cloud Infrastructure Management (Tender Closed)	Where do we keep it? The maintenance and improvement of those data storage services. Management of the overall Azure tenant architecture, its 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 (Tender Closed)	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 Microsoft 365, Azure and other Cloud Services from any location.
Service Desk (Tender Closed)	Who do I call when it breaks? Service Desk is critical to 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.

4.1 In Scope

The following high-level areas are in scope:

1. Software and Platform as a Service Environments in Microsoft 365 and online Office 365 applications



2. Collaboration Tools, including Microsoft Exchange, Teams and SharePoint Online
3. Microsoft Power Platform (Power BI, Power Apps and Power Automate)
4. Azure and Windows Active Directories
5. Identity Integration and access to third party services

4.2 Out of Scope

1. Support for the following is the responsibility of FSA ODD and development partners:
 - a. Solution, application and database development, bespoke code and repositories.
 - b. Custom Microsoft 365 and Power Platform developments, including individual SharePoint sites, Power Apps and Power BI solutions.
2. Deployment and updating of the desktop and mobile editions of Office 365 applications (including WVD specific editions) is supported by the Endpoint Management supplier, as is the support of client hardware and Operating Systems.
3. Active Directory user account administration will be the responsibility of the Service Desk.
4. ServiceNow application, support, maintenance, and licenses. The FSA has its own ServiceNow instance which is supported and maintained.

4.3 Constraints

1. Due to Covid-19 emergency restrictions on occupancy, distancing and travel, access to our offices is likely to be restricted in the short to medium term.

5 Business Requirements

5.1 Overview

The FSA requires a Support Partner to provide end to end management of its cloud hosted business services and directory services as part of a cloud first IT Architecture, ensuring the accessibility, performance and continual improvement of services across a lifecycle geared towards the needs of users in a flexible and mobile-working environment.



The Support Partner will need to work in 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.

5.2 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.

We also provide Services and Active Directory accounts for c700 Operational Contract Staff who are not directly employed by FSA.

5.3 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:

1. Experience of supporting Microsoft 365 and Azure services for UK central or local government customers.
2. Agreement to use FSA's ServiceNow service desk solution as the primary ticketing service and to work with all other disaggregated FSA Support Partners.

6 Operational Requirements

Service	Requirement
1. Microsoft 365	Support and operation of the FSA's Microsoft 365 tenants. This will include initiating the response to Microsoft Service Health notifications, taking the lead role in Incident/ Problem resolution and support escalation with Microsoft when required. (See Error! Reference source not found.). End to end support of the FSA's Exchange 365 environment, including implementation of mail flow



Service	Requirement
	<p>and retention policies, management of Shared Mailboxes, support for Outlook online, desktop and mobile and integration with bulk mail services (e.g., SendGrid, Notify).</p> <p>Support for Email Security, including incident management of SPAM/Phishing, DMARK and SPF record Management, and Bulk email campaigns.</p> <p>Support and operation of the Microsoft Teams platform and, on completion of current support contracts in October 2022, the Microsoft Teams Telephony service.</p> <p>End to end support for the SharePoint platform in the FSA's M365 tenant, which hosts Teams sites, Hub structures and custom site developments. Support for individual SharePoint sites and applications is not included.</p> <p>Support for Retention Policies and Records Management solutions in Microsoft 365.</p> <p>Manage the security of the M365 environment, including day to day monitoring and operation of the Microsoft Defender suite of products.</p>
2. Windows and Azure Active Directory	<p>Support and operate Domain Controllers and ensure that the Windows OS and AD Function Level are maintained to a minimum N-1 standard.</p> <p>(There are currently 4 Domain Controllers hosted in Azure, all running Windows Server 2019 at Function Level Windows 2016.)</p> <p>Configure and manage AD trusts, sites, subnets and FSMO roles.</p> <p>Work collaboratively with the Connectivity partner to ensure that DNS servers are fully operational.</p> <p>Support, operation and optimisation of AD Connect between the Windows and Azure AD, ensuring</p>



Service	Requirement
	<p>that user logon services are available and that account details are refreshed and synchronised.</p> <p>The Service Desk will be responsible for administration of AD user accounts, but the CSM partner will monitor the use of guest user accounts and advise FSA of risks and exceptions (e.g., aged guest accounts) and provide assurance of the integrity of Azure AD Allow and Deny Lists.</p> <p>Conditional Access</p>
3. Business Intelligence and Analytics Tools	<p>Provide support for the underpinning Microsoft Power Platform technologies (PowerBI, PowerApps, Power Automate), ensuring that the toolsets and portals are available, secured and backed up. (Please note that support for individual Power Platform applications, reports and other custom functionality is not included).</p> <p>Proactively monitor performance, respond to and fix anomalous patterns and service outages and undertake Root Cause Analysis.</p>
4. Support for Third Party Services	<p>Work with suppliers of third-party applications in Gartner Layer 1: Systems of Record (See Error! Reference source not found. for applications in scope), to ensure that FSA users are able to access – and securely authenticate with – the applications.</p> <p>Work with FSA and other support partners to design and implement cross-functional solutions in response to changes to third-party hosted services. This will include working in partnership with our Cloud Infrastructure and Connectivity Management partners to enable user access to Government Services as these are migrated from</p>



Service	Requirement
	the Public Sector Network (PSN) to Internet hosting.
5. Lifecycle Management	<p>Enable FSA to make the best use of Microsoft releases and improvements by working with us to plan and implement the release of new and updated M365 services. This will include working with our Endpoint Management partner to ensure that relevant new releases are available for deployment through Intune and other distribution media.</p> <p>Proactively advise FSA of forthcoming end of support deadlines for application and infrastructure components and take a lead role in projects to upgrade or decommission legacy technologies and services.</p> <p>Work with Application Support and Development Partners to ensure that best practice is followed, hosted service capabilities are utilised and re-used and that bespoke solutioning is minimised.</p>

7 Transformation Requirements

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

Service	Requirement
1. Software and Platform as a Service Environments	FSA has an ultimate objective of a Zero Server infrastructure for business services. We are looking for a Cloud Service Management partner to provide infrastructure and platform support for



Service	Requirement
	<p>our in-house teams on projects to migrate applications from IaaS virtual servers to PaaS or SaaS solutions.</p> <p>In parallel, we are pursuing a “buy, don’t build” strategy and are looking for The CSM Support Partner to provide infrastructure and platform support, along with market intelligence and best practice guidance, to projects for replacing bespoke applications with off-the-shelf SaaS services. This will focus on Microsoft 365 and Power Platform but can include other cloud services.</p> <p>As FSA extends the use of M365 and SharePoint for document management, we will be looking to our CSM partner to take an increased role in Information Protection services within M365, including the configuration and implementation of DLP Policies, Compliance attentions, information/Sensitivity Labels, Message Encryption and information rights management.</p>
2. Collaboration Tools & Email	<p>Our current Exchange infrastructure is primarily M365 but contains a hybrid management server. As an on-boarding project, we are looking to the CSM partner to update, as much as possible, to a 365 only email architecture.</p>
3. Windows and Azure Active Directories	<p>The CSM partner will work with FSA to progress our strategic objective of moving from a hybrid AD architecture to an Azure AD First (and ultimately Azure Only) model.</p> <p>This will require The CSM Support Partner to work with us on an initial project to clear up legacy “clutter” in both the Windows and Azure ADs.</p>
4. Technology Roadmap	<p>Support and provide technical leadership of projects and programmes to deliver the FSA’s Technology</p>



Service	Requirement
[See FS430634_015 ODD IT Evergreen Technology Roadmap]	<p>roadmap and work alongside FSA and our support partners to develop portfolios and project plans for implementing our cloud strategy. (Note: we are not seeking costed plans for project delivery, but an understanding of the approach and methodologies and also the process by which project resource can be rapidly assigned).</p> <p>Provide subject matter expertise to help FSA identify how cloud services can be extended without significantly increasing the Total Cost of Ownership.</p> <p>Work with FSA, and provide pro-active expertise, to identify opportunities for roadmap development and enhancement resulting from business change and industry innovations.</p> <p>Enable the above by participating in quarterly (as a minimum) Technology Review meetings with FSA.</p>

8 Service Requirements

Description	Purpose
1. Resource Management	<p>Proactively manage the scope of the Operational and Transformation Requirements to balance peaks and troughs of FTE activity and prevent additional costs and resource bottlenecks.</p> <p>Define committed lead time to access the more specialist skills and resources, where required.</p>
2. Service Availability	<p>Support will be on a 24/7/365 basis, including core or 'working' hours 7:00am to 8:00pm Monday to Friday, and non-core 8:00pm to 7:00am Monday to Friday plus weekends and bank holidays.</p>



Description	Purpose
3. Accessibility [See FS430634_013 FSA Supplier Access Policy August 2019 v1, FS430634_014 FSA IT Acceptable Use Policy Nov 2020 v3.2]	The CSM Support Partner shall ensure that all services and documentation meet latest WCAG accessibility standards for their area of responsibility.
4. User Access	The CSM Support Partner shall adhere to the FSA User Access policy. Role based user access must be supported and integration with Azure AD.
5. GDPR	The CSM Support Partner must comply with their responsibilities under GDPR.
6. Service Management [See FS430634_006 FSA Acceptance into Service Procedure, FS430634_007 FSA Change Management Procedure, FS430634_008 FSA Incident Management	The CSM 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.



Description	Purpose
<p>Procedure, FS430634_009 FSA Security Incident</p> <p>Procedure 2019, FS430634_010 FSA Problem Management Process,</p> <p>FS430634_011 FSA Knowledge Management</p> <p>Procedure, FS430634_012 FSA Service Asset & Configuration Mgt</p> <p>Procedures, FS430634_016 FSA Request Fulfilment, FS430634_017 Service Level Agreements, FS430634_018 FSA Patching Policy Sept 2019 1.1]</p>	<p>The CSM Support Partner shall provide high- and low-level design documents for all services and solutions within scope of the contract. 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.</p> <p>The CSM Support Partner shall contribute to the review of services, evaluation, definition, execution and monitoring of Continual Service Improvement, ensuring these are appropriately recorded and reported against ITIL principles must be followed.</p> <p>The CSM Support Partner will work on the FSA ServiceNow instance with respect to all service management processes.</p> <p>The CSM 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.</p> <p>The CSM Support Partner will work to Service Level Agreements as specified in the FSA Service Level Agreement document</p>
7. Ways of working	<p>The CSM 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.</p> <p>Work with the FSA Security team to deliver security assurance, including support for and providing input to the requirements for scheduled pen tests.</p>



Description	Purpose
8. Support Partner's End User Devices	<p>The CSM Support Partner shall ensure that: FSA Data which resides on an uncontrolled CSM Support Partner device is stored encrypted through a process agreed with the FSA.</p> <p>Any Device used for FSA data is compliant with NCSC End User Devices Platform Security Guidance</p>
9. Networking	<p>The CSM Support Partner will ensure that any FSA Data which it causes to be transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.</p>
10. Personnel Security	<p>The CSM 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. See attached for further information.</p>
11. Hosting and Location of FSA Data	<p>The CSM Support Partner shall ensure that neither they nor their Sub-contractors will process FSA Data outside the EEA (including backups) without the prior written consent of the FSA.</p>



ITT Qualification questions and responses

QUALIFICATION RESPONSES EVALUATION DETAILS (*)

Number of Responses	1
Number of Questions	26

Supplier		Methods Business & Digital Technology
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	The supplier will have Experience of supporting Microsoft 365 and Azure services for UK central or local government customers.	
	Response	
	Yes	
Question	Description	
1.1.3 2	Service Tools - The supplier will use FSA's ServiceNow service desk solution as the primary ticketing service and work with all other disaggregated FSA Support Partners.	
	Response	
	Yes	
Question	Description	
1.1.4 3	Accessibility - The supplier will ensure that all services and documentation meet WCAG 2.1 AA accessibility standards for their area of responsibility.	



Response	
Yes	
Question	Description
1.1.5 4	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.
Response	
Yes	
Question	Description
1.1.6 5	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.
Response	

Response	
Yes	
Question	Description
1.1.7 6	Security Incident Management - The Supplier will comply with the FSA security incident management policy. All security incidents will be prioritised as a P2 or above.
Response	
Yes	
Question	Description
1.1.8 7	Delivery Manager - The supplier will proved a named Service Delivery Manager.
Response	
Yes	
Question	Description
1.1.9 8	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.
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 1	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.
Response	
Yes	

Question	Description
1.2.3 2	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.
Response	
Yes	

Question	Description
1.2.4 3	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.
Response	
Yes	

Question	Description
1.2.5 4	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.
Response	
Yes	



Question	Description
1.2.6 5	Event Logs, Reporting 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 proactive approach to reviewing these audit records.
Response	
Yes	

Question	Description
1.2.7 6	Hosting and Location of FSA Data - The Supplier shall ensure that they and none of their Sub-contractors Process FSA Data (including data used in the management of the service in their own system) outside the EEA (including backups) without the prior written consent of the FSA. The Supplier must also provide the locations within the EEA where data is stored.
Response	
Yes	

Question	Description
1.2.8 7	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.
Response	
Yes	

Question	Description
1.2.9 8	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 tools and controls to protect the service from malicious software. The supplier will monitor and manage the alerts and if malicious software is found the supplier will be responsible for managing the incident and

Question	Description
1.2.9 8	removal in line with NCSC guidelines.
Response	
Yes	



Question	Description
1.2.10 9	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 ;
Response	
Yes	
Question	Description
1.2.11 10	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
Response	
Yes	
Question	Description
1.2.12 11	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
Response	
Yes	
Question	Description
1.2.13 12	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.
Response	
Yes	
Question	Description
1.2.14 13	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 .
Response	
Yes	
Question	Description
1.2.15 14	Principles of Security - The Supplier has Cyber Essentials PLUS
Response	



Yes

Question	Description
1.2.16 15	Principles of Security - 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 .
Response	
Yes	

Question	Description
1.2.17 16	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.
Response	
Yes	

(*) Filtered suppliers accepted in this report:

- 1) Methods Business & Digital Technology



Operational ITT Response

- | | |
|--------------------|--|
| • TENDER reference | • FS430634 – Cloud Service Management Management |
|--------------------|--|

Section 1: Microsoft 365 – 25%

A Support and operation of the FSA's Microsoft 365 tenants. This will include initiating the response to Microsoft Service Health notifications, taking the lead role in Incident/ Problem resolution and support escalation with Microsoft when required.

Q1 - Please provide an example of your support of Microsoft365 for an organisation similar to FSA. In particular, please describe how the governance and touchpoints with the customer and end users was applied and any lessons learned that you consider relevant to FSA – 15%

[Redacted content]



[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]



[Redacted text block]

B End to end support of the FSA's Exchange 365 environment, including implementation of mail flow and retention policies, management of Shared Mailboxes, support for Outlook online, desktop and mobile and integration with bulk mail services (e.g., SendGrid, Notify).

Q2 - Outline your experience of supporting Exchange 365 and your management of mailbox, routing and other policies for an organisation of similar size to FSA – 15%

[Redacted text block]



Crown
Commercial
Service



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

C Support for Email Security, including incident management of SPAM/Phishing, DMARK and SPF record Management, and Bulk email campaigns.

Q3 - How will you manage Email security (e.g. SPAM/Phishing emails), DMARK and SPF record Management, and Bulk email campaigns and respond to security alerts and incidents? – 10%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text line]

[Redacted text block]

• [Redacted text line]

[Redacted text block]

[Redacted text block]

• [Redacted text line]

[Redacted text block]

[Redacted text block]

• [Redacted text line]

[Redacted text block]

[Redacted text block]

• [Redacted text line]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

o



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

D Support and operation of the Microsoft Teams platform and, on completion of current support contracts, the Microsoft Teams Telephony service.

Q4 - Describe how you will ensure the integrity of the Microsoft Teams platform and work alongside FSA to prevent and correct "Teams Bloat" through uncontrolled customisation – 10%

[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]

RM3804 Order Form v4 - August 2019



[Redacted text block]

[Redacted text block]

Q5 - What will be your approach to taking on support for Teams Telephony when the current support contract expires? (Note: FSA uses Direct Routing) – 10%

[Redacted text block]



[Redacted content]



- [REDACTED]

E End to end support for the SharePoint platform in the FSA's M365 tenant, hosting Teams sites, Hub structures and custom site developments. Support for individual SharePoint sites and applications is not included.

Q6 - Please describe your experience of supporting the SharePoint on-line platform and how will you work with FSA and development partners to maintain the integrity of the platform while enabling the deployment of new sites and applications – 10%

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]



Figure 1



[Redacted content]



- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

F Support for Retention Policies and Records Management solutions in Microsoft 365.

Q7 - How will you ensure that FSA's Records Management and Retention policies are applied effectively consistently across the M365 tenant? – 10%

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]





[Redacted text block]

[Redacted text line]

[Redacted text line]

- [Redacted text line]
- [Redacted text line]
- [Redacted text line]
- [Redacted text line]

[Redacted text line]

- [Redacted text line]
- [Redacted text line]
- [Redacted text line]
- [Redacted text line]
- [Redacted text line]

G Manage the security of the M365 environment, including day to day management of the Microsoft Defender suite of products

Q8 - Can you please describe how you will provide protective monitoring of M365 service to monitor and protect against the latest and emerging security threats and vulnerabilities? – 10%

[Redacted text block]

[Redacted text block]

A series of horizontal bars, mostly blacked out, with some blue dots visible on the left side. The bars are of varying lengths and are arranged in a vertical sequence. The blue dots are small and appear to be markers or indicators on the left edge of the bars.



• [Redacted]
[Redacted]
[Redacted]
• [Redacted]
[Redacted]

Q9 - FSA will be upgrading all M365 subscriptions from E3 with Add-Ins to E5; how will you work with us to realise the security benefits of the upgrade and, in particular, to implement Defender for Office proactively to ensure that policies and baselines are configured for operational efficiency as well as compliance? – 10%

[Redacted]

[Redacted]

[Redacted]

• [Redacted]
• [Redacted]
• [Redacted]
• [Redacted]



[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

- [Redacted]

Section 2: Windows and Azure Active Directory – 25%

**A Support and operate Domain Controllers and ensure that the Windows OS and AD Function Level are maintained to a minimum N-1 standard.
Configure and manage AD trusts, sites, subnets and FSMO roles.**

Q10 - Describe your experience of managing the Windows Active Directory architecture (domains, sites, subnets) for a customer similar to FSA. Please make particular reference to how you ensured that domain controllers and the AD Function Level were upgraded to maintain currency with Windows Server releases – 35%



[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[illegible]



Q11 - Overall responsibility for FSA's DNS infrastructure sits with our Connectivity provider; however, you will be responsible for the Domain Controllers which provide internal DNS. How will you work with the Connectivity provider to ensure that the server infrastructure is correctly configured and to collectively resolve DNS issues – 25%

[illegible]



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

C The Service Desk will be responsible for administration of AD user accounts, but the CSM partner will monitor the use of guest user accounts and advise FSA of risks and exceptions (e.g. aged guest accounts) and provide assurance of the integrity of Azure AD Allow and Deny Lists.

Q12 - How will you provide assurance to FSA that external access to M365 and Azure services (in particular Teams and SharePoint sites) is configured appropriately to meet both security and information sharing requirements – 15%

[Redacted]

[Redacted]

[Redacted]

• [Redacted]

• [Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

• [Redacted]

• [Redacted]

[Redacted]

• [Redacted]

○ [Redacted]



Crown
Commercial
Service

[illegible]



[Redacted text block]

D Support, operation and optimisation of AD Connect between the Windows and Azure AD, ensuring that user logon services are available and that account details are refreshed and synchronised.

Q13 - Describe how you have implemented and managed the AD Connect service for a customer similar to FSA. In particular, what tools and approaches have you used to ensure that the service is both optimised and fully resilient? – 25%

[Redacted text block]



[Redacted text block]

[Redacted text block]

- [Redacted text block]

- [Redacted text block]

- [Redacted text block]

- [Redacted text block]

[Large redacted text block]

[Redacted text block]

- [Redacted text block]

[Redacted text block]

- [Redacted text block]



[Redacted content]

Section 3: Business Intelligence and Analytics Tools - 20%

- **A Provide support for the underpinning Microsoft Power Platform technologies (PowerBI, PowerApps, Power Automate), ensuring that the toolsets and portals are available, secured and backed up. (Please note that support for individual Power Platform applications, reports and other custom functionality is not included).**
- Q14 - Describe how you will support the Microsoft Power Platform environment. What would you see as the required operational tasks and what steps would you take to resolve performance issues reported to the service desk by application users? – 50%



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



- **B Proactively monitor performance, respond to and fix anomalous patterns and service outages and undertake Root Cause Analysis.**
- Q15 - Give an example to illustrate your experience of performance monitoring and problem resolution in respect of Microsoft Power tools. How have you engaged with application operations and development providers to accomplish this? -50%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



Section 4: Support for Third Party Services - 15%

A Work with suppliers of third party applications in Gartner Layer 1: Systems of Record to ensure that FSA users are able to access – and securely authenticate with – the applications.

Q16 - Scenario: A third party hosted service has been upgraded and users report that they "cannot log on to the application". User accounts are synchronised with your customer's Windows AD through ADFS. How will you work with the service provider to troubleshoot the issue and ensure that resolution is assigned to the appropriate partner? – 50%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]



[Redacted text block containing multiple lines of blacked-out content]

[Redacted text block containing multiple lines of blacked-out content]

[Redacted text block containing a single line of blacked-out content]

[Large redacted text block covering the bottom half of the page]



[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

B Work with FSA and other support partners to design and implement cross-functional solutions in response to changes to third-party hosted services, In particular, this will include working in partnership with our Cloud Infrastructure and Connectivity Management partners to enable user access to Government Services as these are migrated from the Public Sector Network (PSN) to Internet hosting.

Q17 - How will you work with both FSA and our Cloud Infrastructure and Connectivity Management partners to enable user access to Government Services as these are migrated from the PSN to Internet hosting? – 50%

[Redacted]



[REDACTED]

• [REDACTED]

• [REDACTED]

• [REDACTED]

• [REDACTED]

1. **Identify the main components of the system.**
 2. **Define the scope and objectives of the project.**
 3. **Develop a detailed project plan.**
 4. **Implement the plan and monitor progress.**
 5. **Evaluate the results and provide feedback.**

Section 5: Lifecycle Management – 15%



A. Enable FSA to make the best use of Microsoft releases and improvements by working with us to plan and implement the release of new and updated M365 services. This will include working with our Endpoint Management partner to ensure that relevant new releases are available for deployment through Intune and other distribution media.

Q18 - Our objective is to make sure that as Microsoft release and update 365 services, we are able to identify those that will have the greatest user benefit and impact. Please describe how you will bring understanding of the M365 services and the release schedules to proactively inform FSA and our support partners' release management processes – 40%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

B Work with Application Support and Development Partners to ensure that best practice is followed, hosted service capabilities are utilised and re-used and that bespoke solutioning is minimised.

Q19 - How will you work with Application Support and Development Partners to ensure that best practice is followed, that hosted service capabilities are utilised and re-used and that bespoke solutioning is minimised? – 30%

[Redacted]

[Redacted]

[Redacted]

[illegible]



[Redacted content]

C Proactively advise FSA of forthcoming end of support deadlines for application and infrastructure components and take a lead role in projects to upgrade or decommission legacy technologies and services.

Q20 - How will you ensure that end of life/ end of support notifications are acted upon and that FSA are appraised of the options for addressing them? – 30%

[Redacted content]

[Redacted content]

[Redacted content]



[Redacted content]

[illegible]



• [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 text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted text block]
- [Redacted text block]
- [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



- [REDACTED]
- [REDACTED]
- [REDACTED]

B In parallel, we are pursuing a “buy, don’t build” strategy and are looking for The CSM Support Partner to provide infrastructure and platform support, along with market intelligence and best practice guidance, to projects for replacing bespoke applications with off-the-shelf SaaS services. This will focus on Microsoft 365 and Power Platform, but can include other cloud services.

Q2 - How will you provide market intelligence to inform the replacement of bespoke applications with SaaS services? – 20%

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]



- [Redacted]
 - [Redacted]
- [Redacted]
- [Redacted]
 - [Redacted]

Q3 - How will you approach solution migration, and what techniques will you employ to prototype and test new solutions - in particular those created using Microsoft 365 and Power Platform - and to ensure that the "Buy, Don't Build" principle is being followed? – 30%

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

o



[Redacted]

C As FSA extends the use of M365 and SharePoint in particular for document management, we will be looking to our CSM partner to take an increased role in Information Protection services within M365, including the configuration and implementation of DLP Policies, Compliance attentions, information/Sensitivity Labels, Message Encryption and information rights management.

Q4 - Please describe your experience of supporting Information Protection (DLP Policies, Compliance attentions, information/Sensitivity Labels, Message Encryption and information rights management) for an organisation similar to FSA – 20%

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

RM3804 Order Form v4 - August 2019



Crown
Commercial
Service

[illegible]



Section 2: Collaboration Tools & Email - 25%

A Our current Exchange infrastructure is primarily M365, but contains a hybrid management server. As an initial project, we're looking to the CSM partner to update to a 365 only email architecture.

Q5 - Give an example of how you have migrated an organisation's email from a hybrid infrastructure to Exchange 365. What issues did you encounter and how were they overcome? – 100%

Please note: the initial hybrid migration project should not be included in the baseline costs, but we do require a stand-alone project cost for this.

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]



[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]



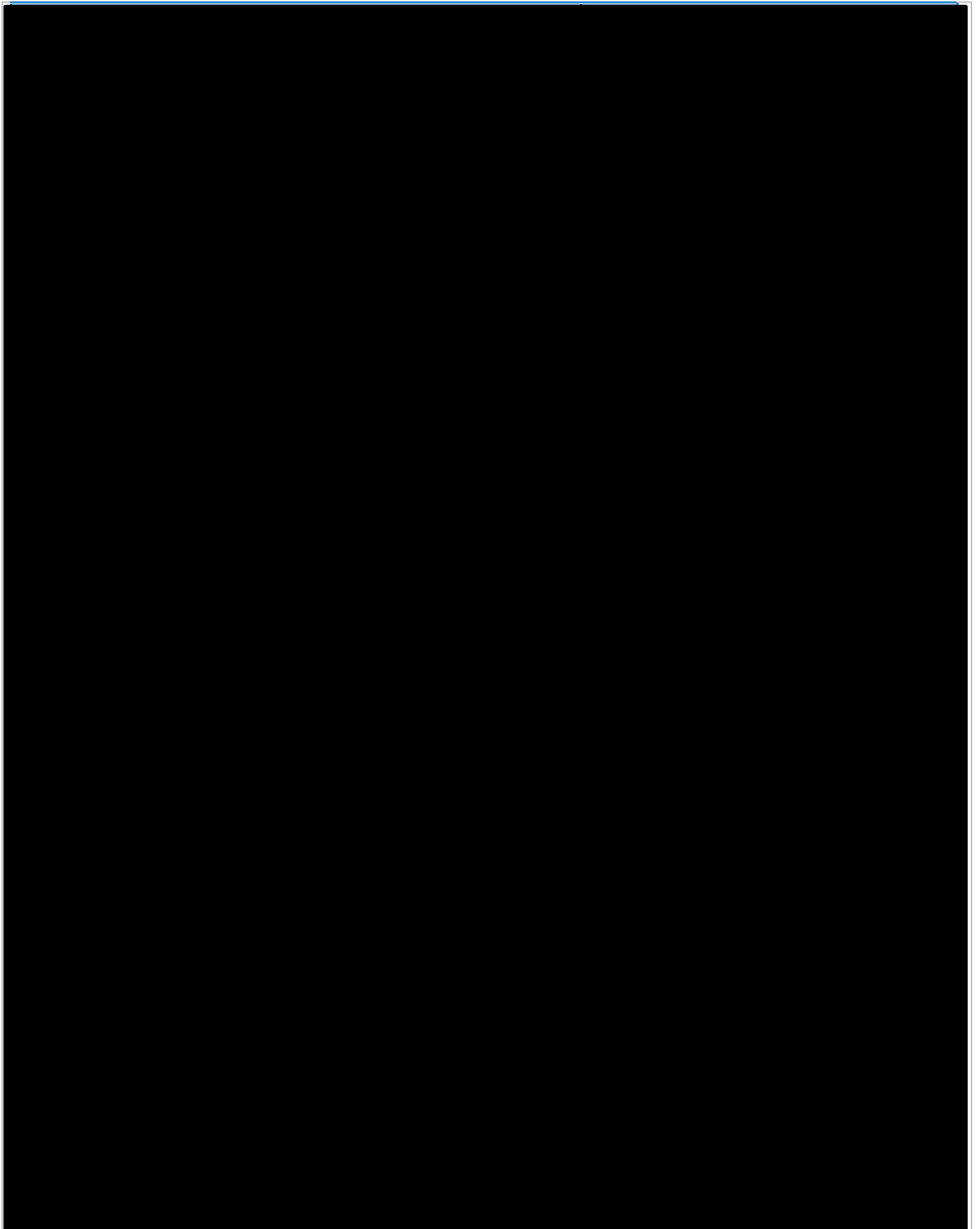
[Redacted text block]

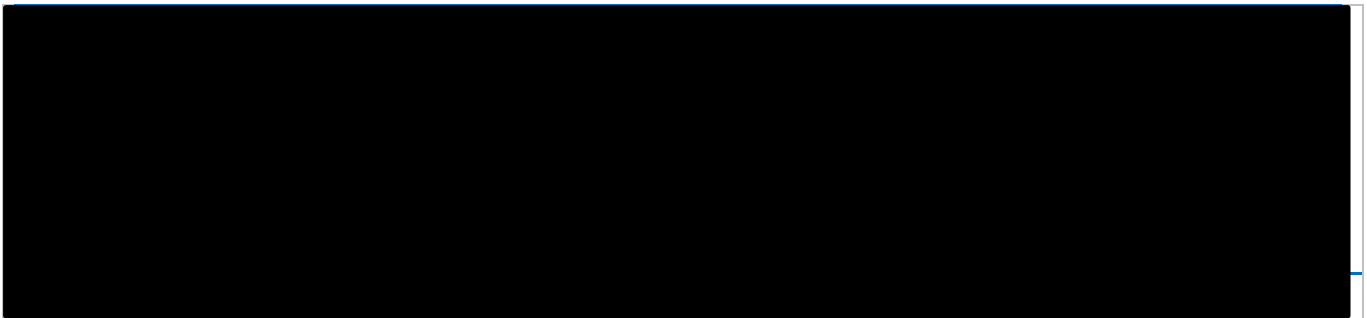
[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]





Section 3: Windows and Azure Active Directories - 25%

- 8.10 A The CSM partner will work with FSA to progress our strategic objective of moving from a hybrid AD architecture to an Azure AD First (and ultimately Azure Only) model. This will require The CSM Support Partner to work with us on an initial project to clear up legacy "clutter" in both the Windows and Azure ADs
- 8.11 Q6 - FSA has a strategic objective to transform from an Azure/ On-Premises AD hybrid to Azure AD only. What do you see as the pre-requisites, milestones and potential blockers and how will you work proactively and collaboratively with us to deliver the strategy over the lifecycle of the contract? – 100%
- 8.12
- 8.13 Please note: the initial legacy clean-up project should not be included in the baseline costs, but we do require a stand-alone project cost for this.





[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Section 4: Technology Roadmap – 25%

A Support and provide technical leadership of projects and programmes to deliver the FSA's Technology roadmap and work alongside FSA and our support partners to develop portfolios and project plans for implementing our cloud strategy.

(Note: we are not seeking costed plans for project delivery, but an understanding of the approach and methodologies and also the process by which project resource can be rapidly assigned).

Q7 - Describe your approach to project delivery and how you will provide technical leadership to cross-supplier project teams – 30%

[Redacted text block]



[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

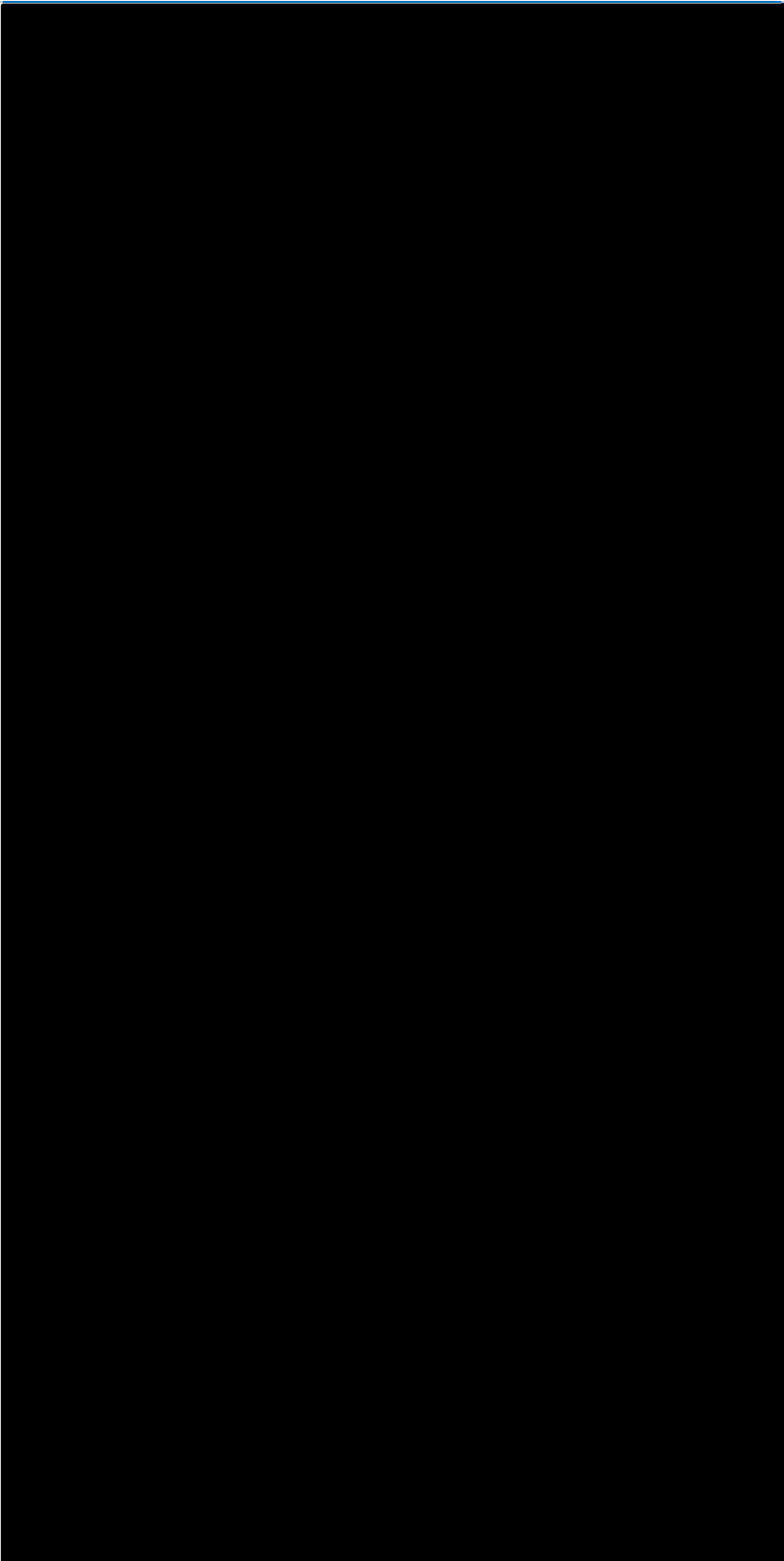
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]





[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

- [Redacted list item]



[Redacted text block]

[Redacted text block]

B Provide subject matter expertise to help FSA identify how cloud services can be extended without significantly increasing the Total Cost of Ownership.

Q8 - FSA is seeking to expand our use of cloud services in a way that helps reduce the Total Cost of IT Ownership in the organisation. Please describe how you have supported a similar organisation in achieving this objective – 30%

[Redacted text block]

- [Redacted text block]

[Redacted text block]

- [Redacted text block]



The diagram consists of four horizontal bars of varying lengths, arranged vertically. Each bar has a small blue dot at its left end. The bars are arranged such that the top bar is the longest, and each subsequent bar below it is shorter than the one above it. A red circle is positioned below the bottom-most bar, to the left of its left end.



○

○

●

○

C 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 participating in quarterly (as a minimum) Technology Review meetings with FSA.

Q9 - Describe your roadmap for delivery of service improvements in cloud technologies and services delivery over the next 12-24 months, including how new services will be made available to the FSA – 40%

●

●

●

●

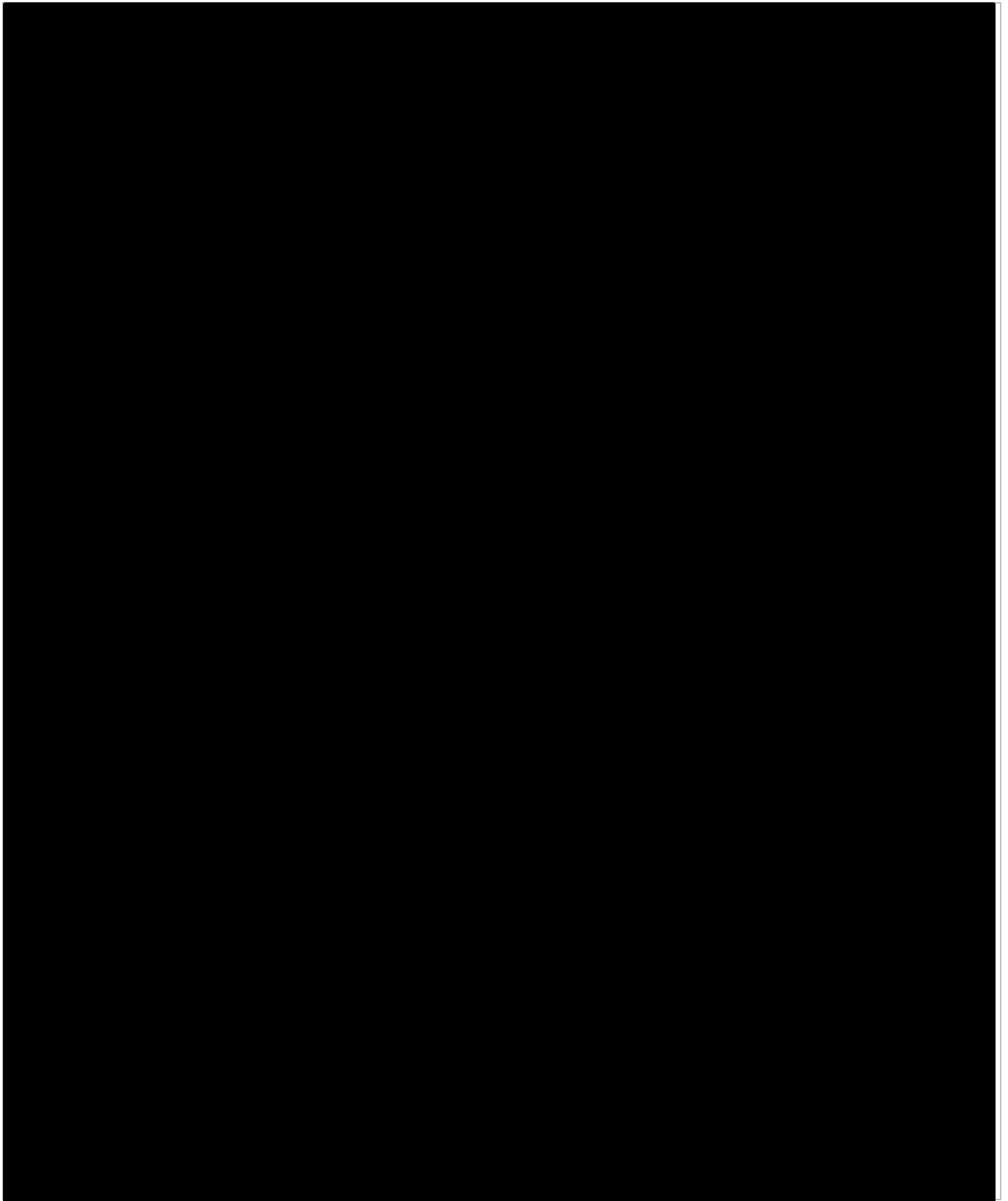
●

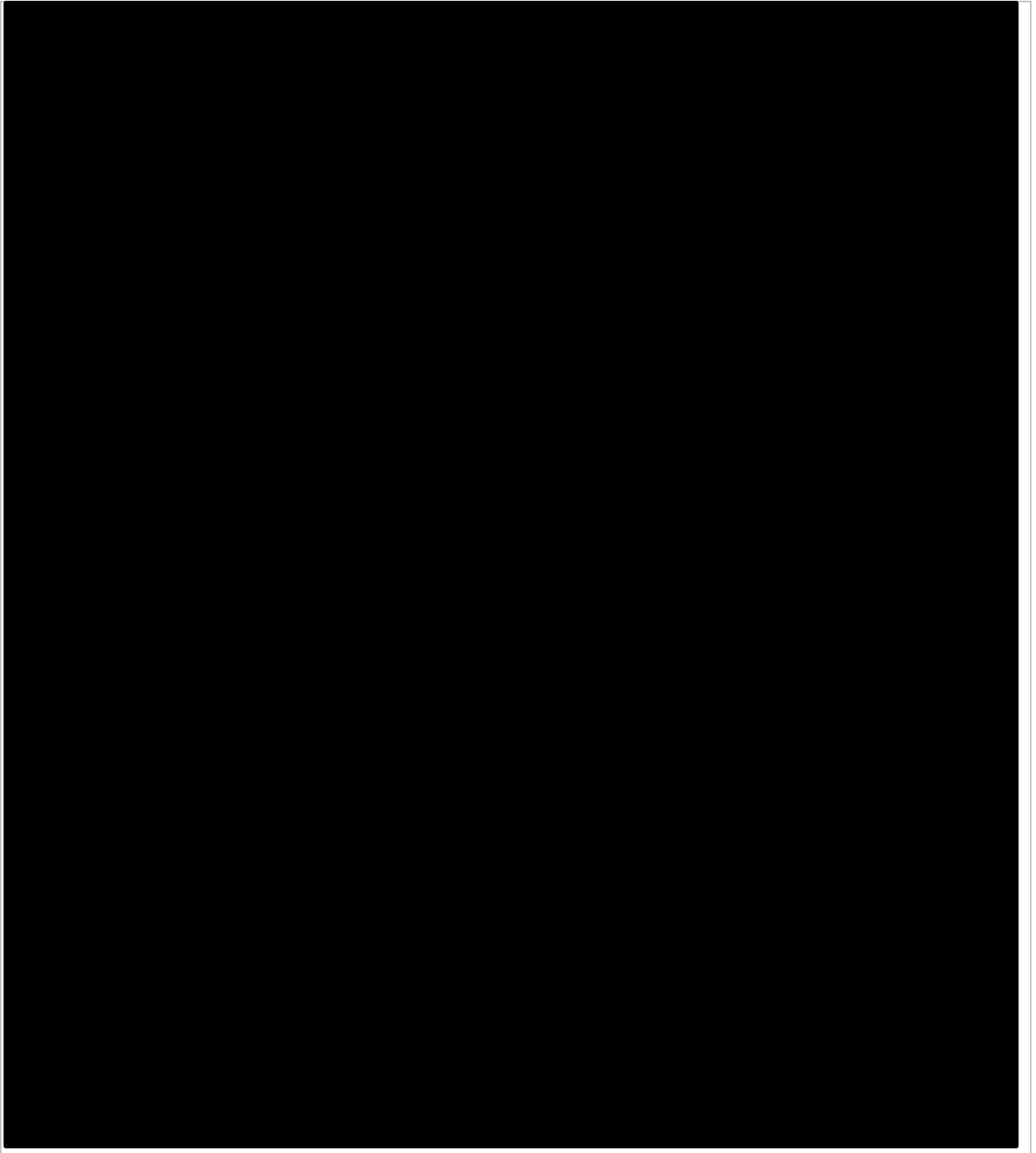
●



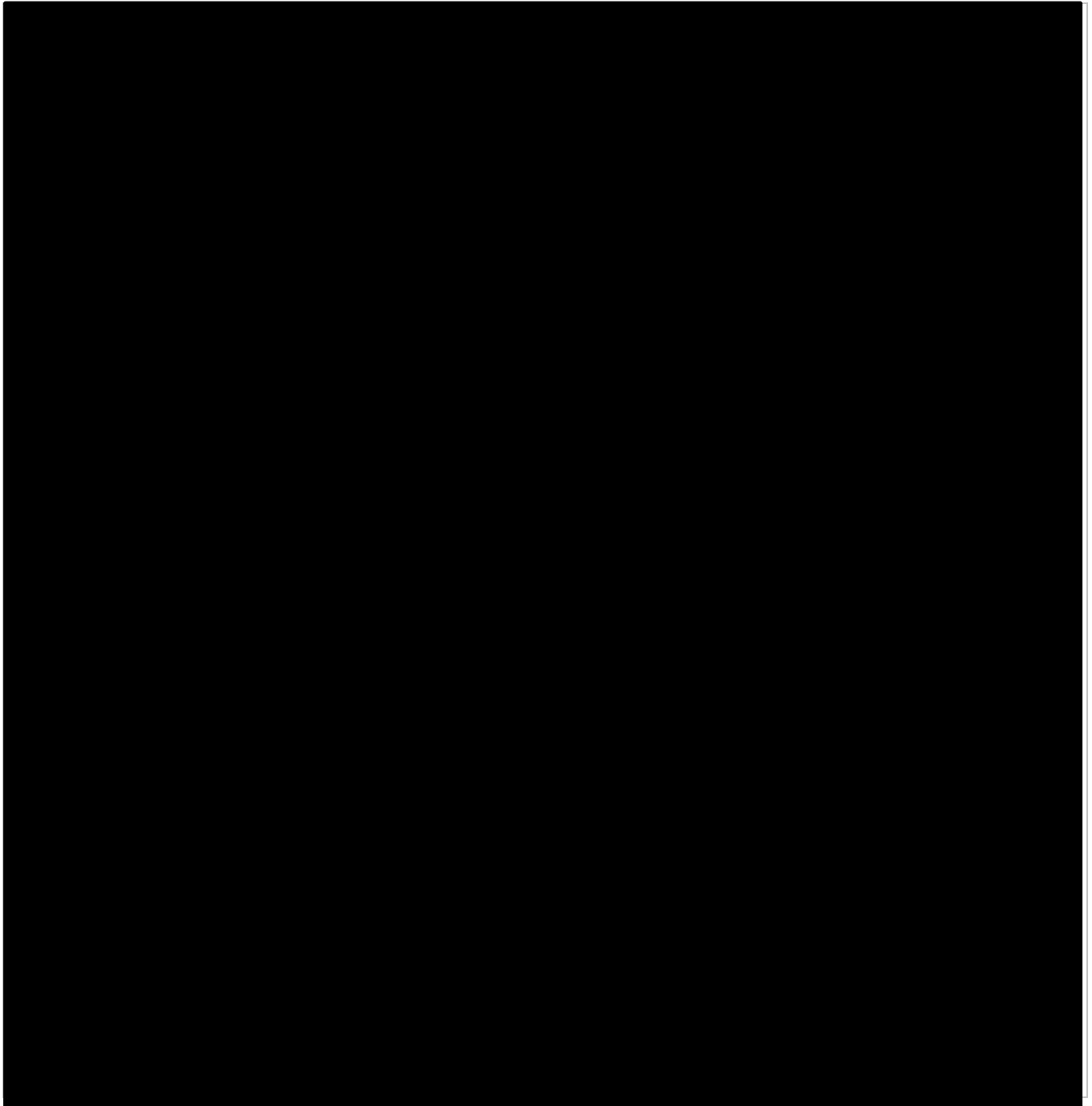
[Redacted text block]

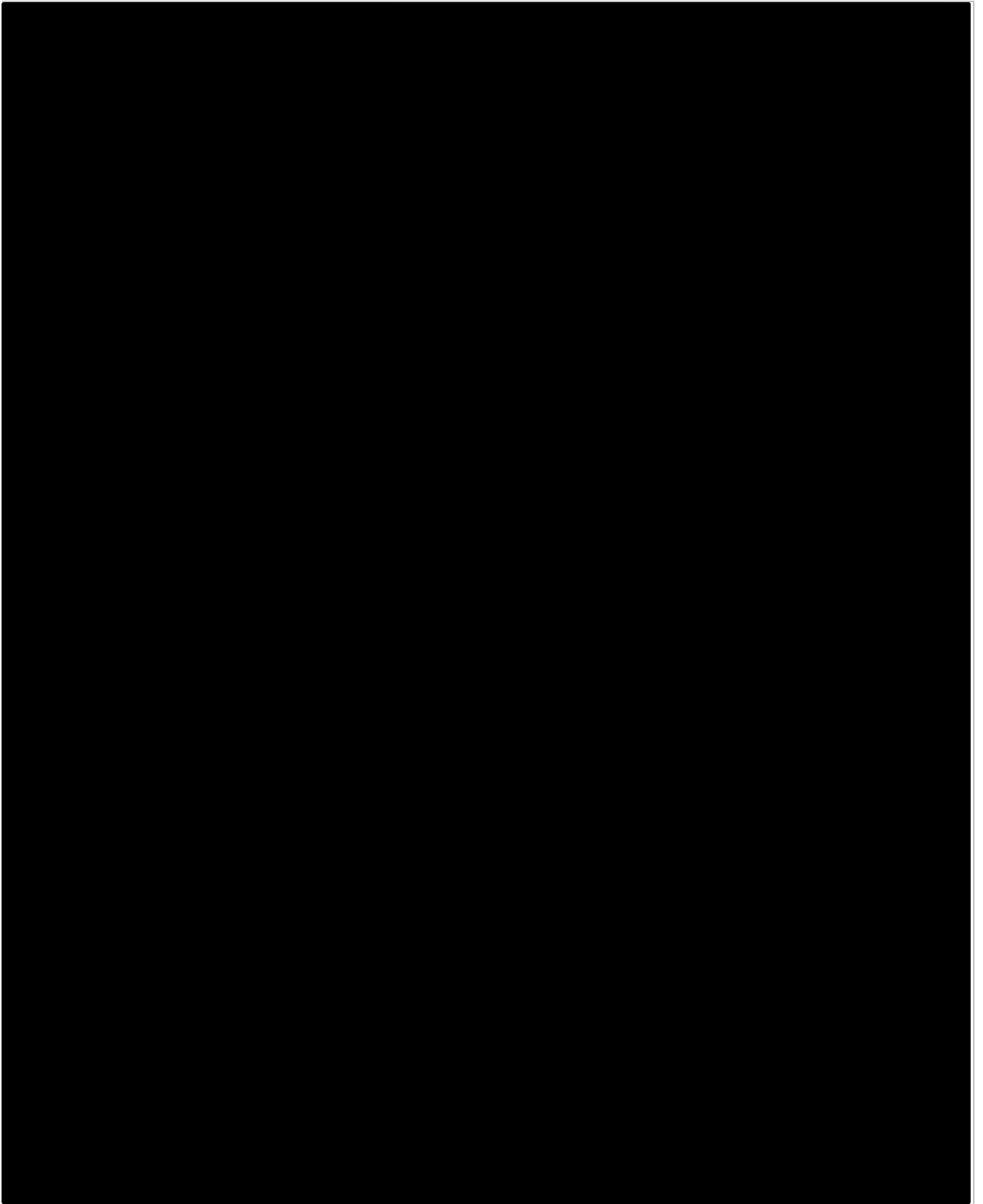
[Redacted text block]













[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

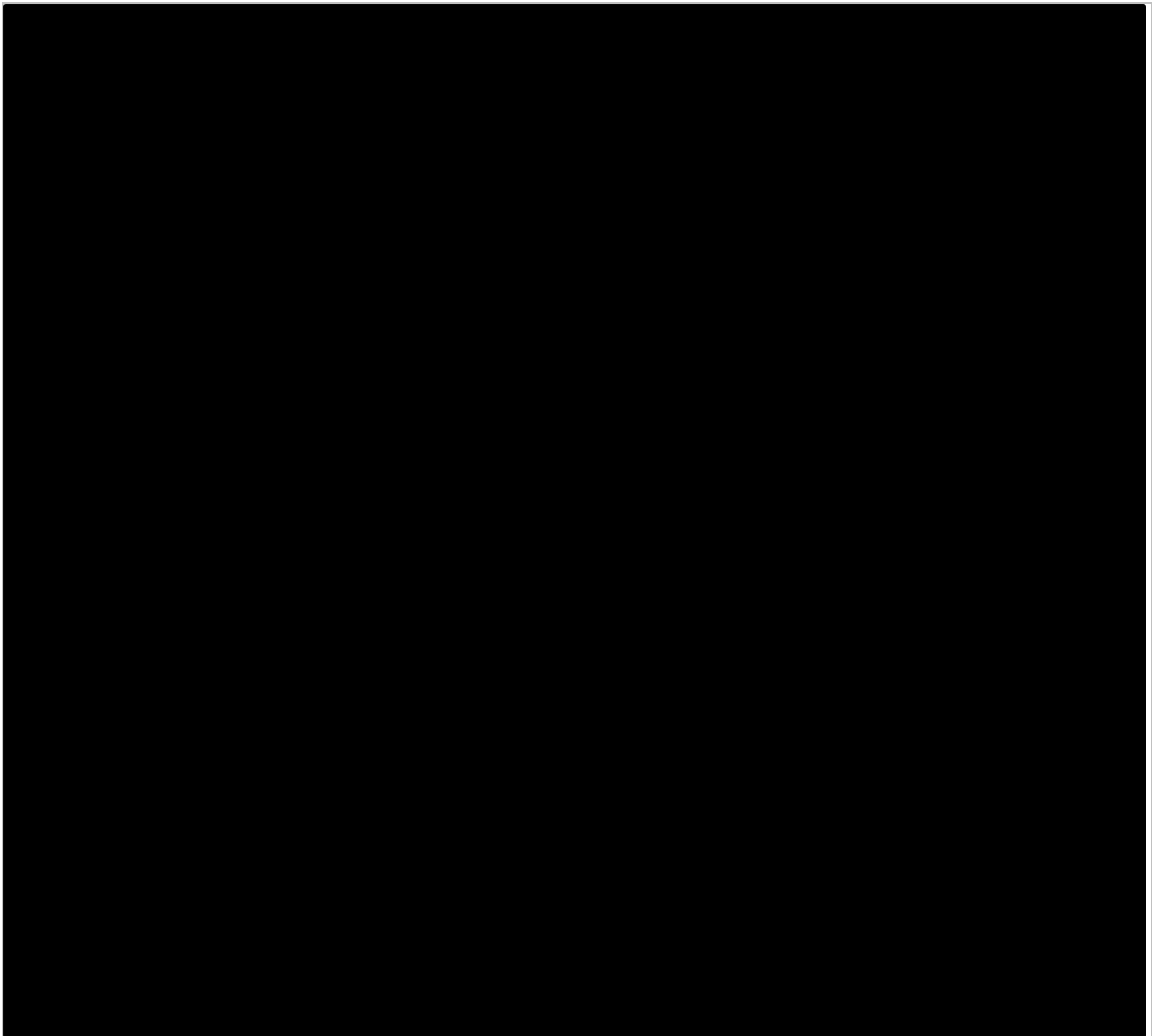


Service ITT Response

[illegible]



[Redacted content]



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]

[Redacted]



Q3 - Describe your own processes for the acceptance of new services, and how these ensure you are able to provide appropriate support. Please include your own process flows/diagrams in your answer – 10%

A stylized illustration of a city skyline at night. The scene is composed of various geometric shapes representing buildings and structures. The color palette is primarily dark blue and black, with highlights in white and light blue. The buildings are of different heights and widths, creating a sense of depth and perspective. Some buildings have small, glowing windows, adding to the nighttime atmosphere. The overall style is modern and minimalist, with a focus on the silhouettes and light patterns of the city.



[Redacted text block]

[Redacted text block]

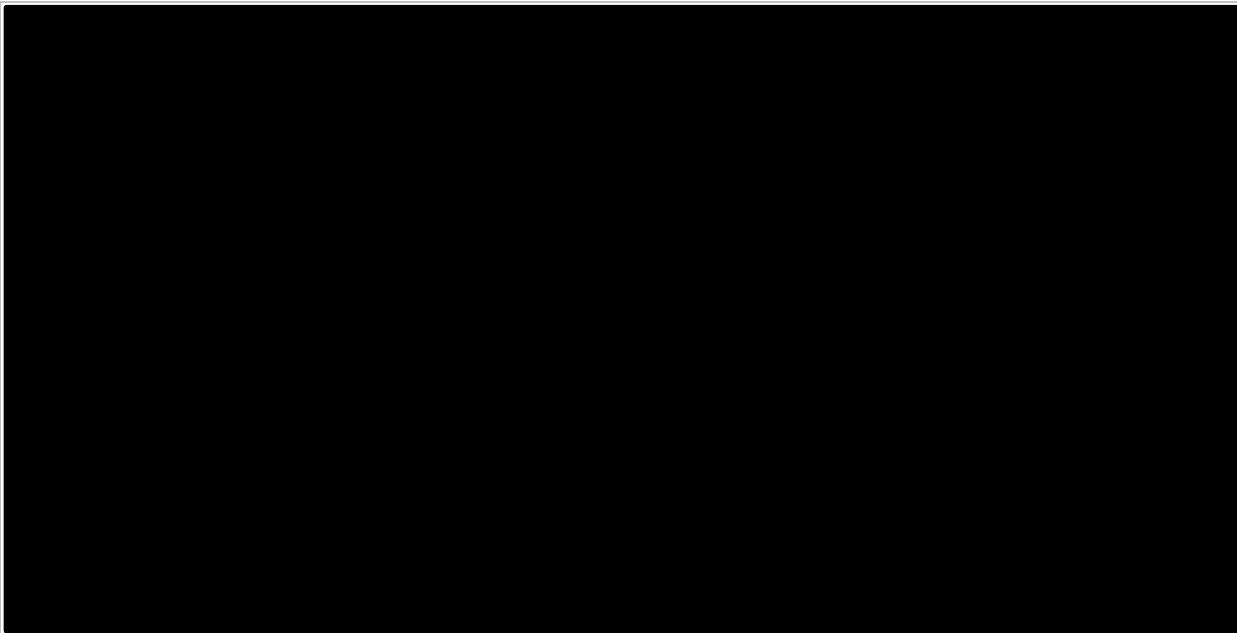
D Change management - The supplier shall work to the FSA change management process, and contribute to the assessment, logging, review, implementation, scheduling, review and closure of changes.

Q4 - Describe your approach to change management and what actions you take to minimize the risks associated with changes. Please feel free to include any diagrams/process flows into your answer – 5%

[Redacted text block]



RM3804 Order Form v4 - August 2019



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 how you produce design documentation and how you ensure that documents are accurate and up-to-date. Please provide examples of design documentation content/format – 5%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text]

[Redacted text]

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. Please feel free to include any diagrams/process flows into your answer – 15%

[Redacted text]



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Large redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

G 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 ensuring the knowledge base is up-to-date and accurate for the services they support.

Q7 - Describe your approach to knowledge management and how you ensure that documents and Knowledge Base articles are accurate and up-to-date. – 10%

[Redacted]



Age Group	Gender	U.S. should take action (%)	U.S. should not take action (%)
18-29	Male	88	12
	Female	85	15
30-49	Male	82	18
	Female	78	22
50-69	Male	75	25
	Female	70	30
70+	Male	68	32
	Female	65	35



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

H 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.

Q8 - Explain your approach to a monthly performance reports and how you would highlight issues or areas of concern – 3%

[REDACTED]

[REDACTED]



Crown
Commercial
Service

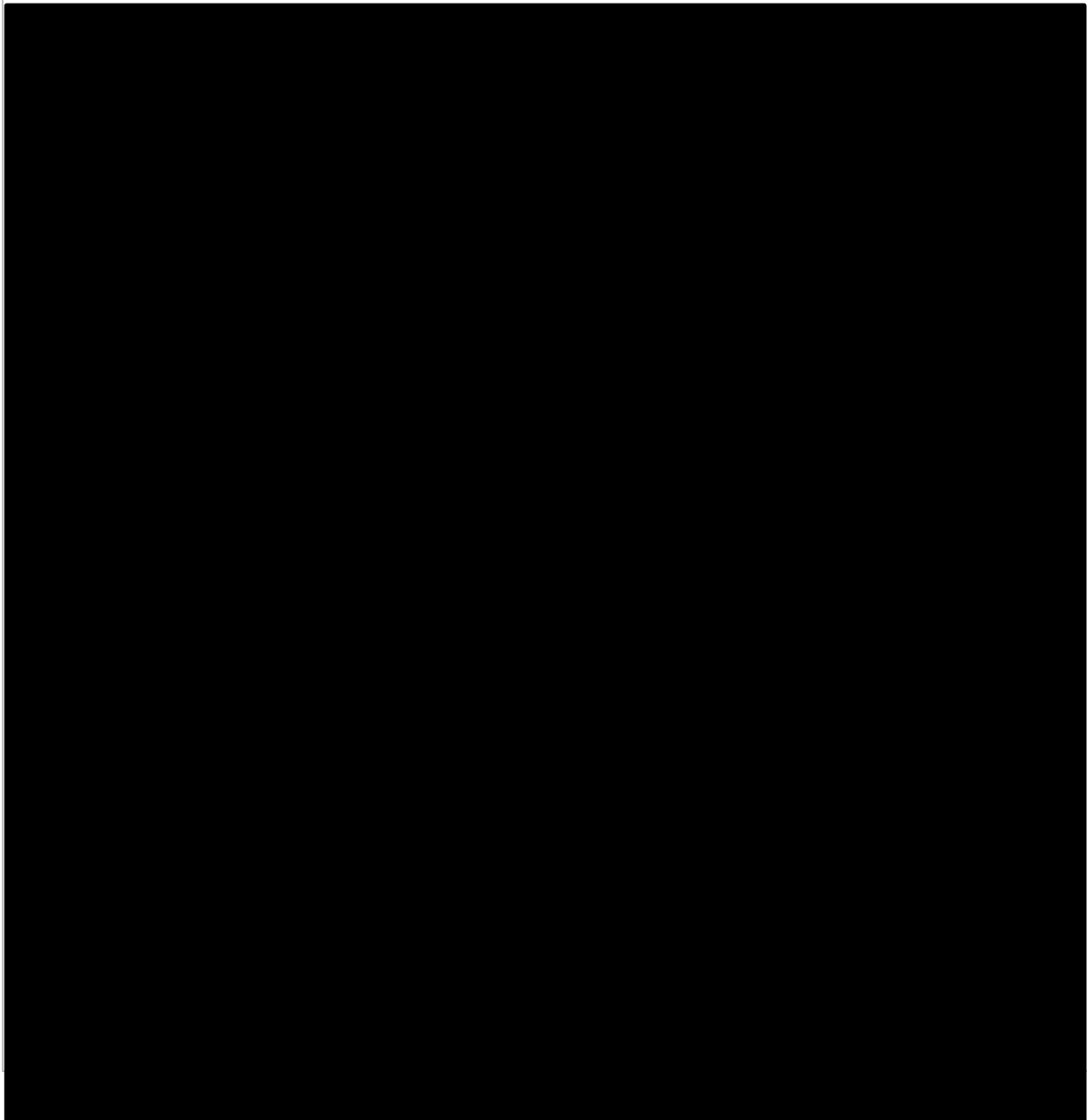
■ [REDACTED]



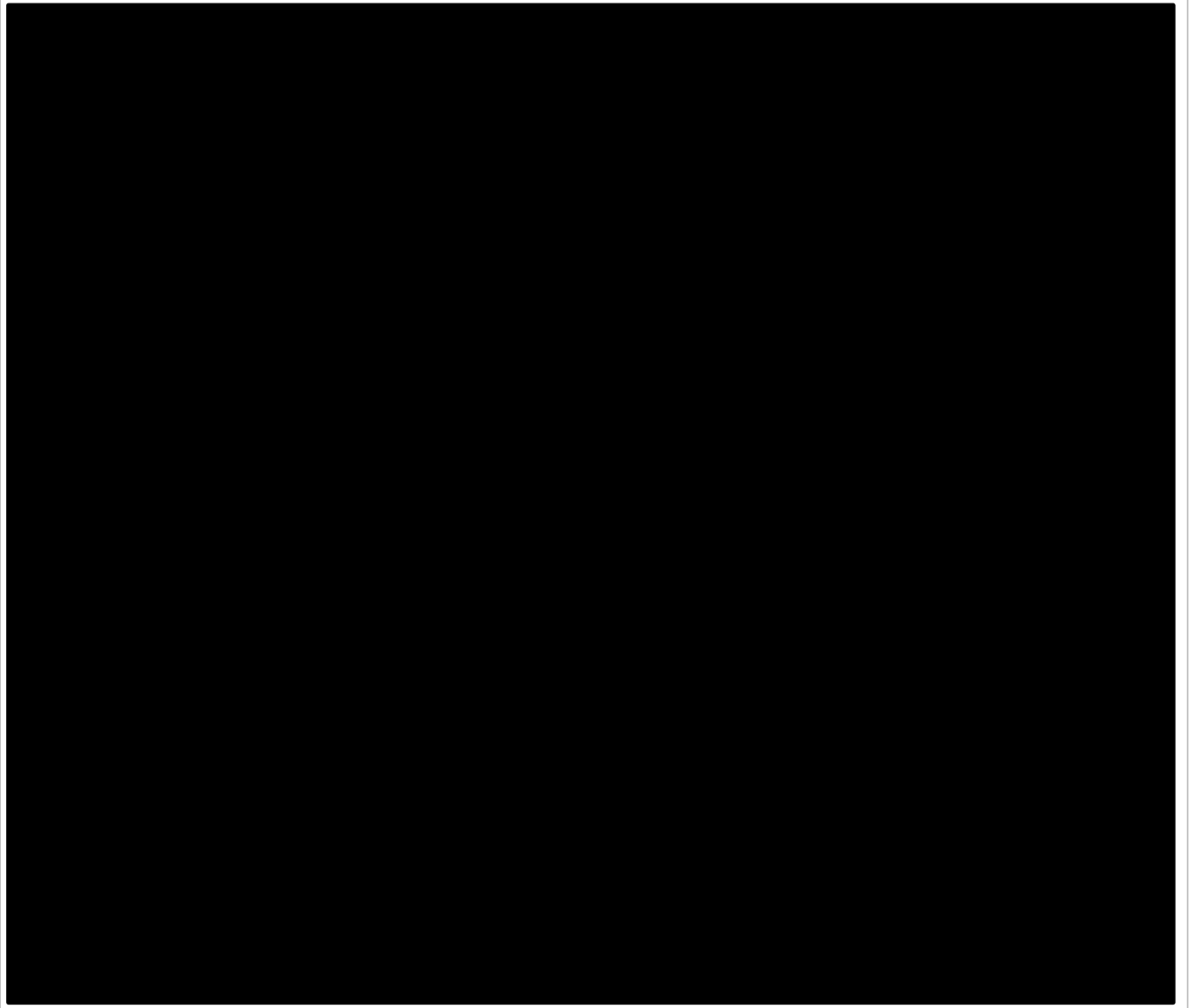
[Redacted text block]

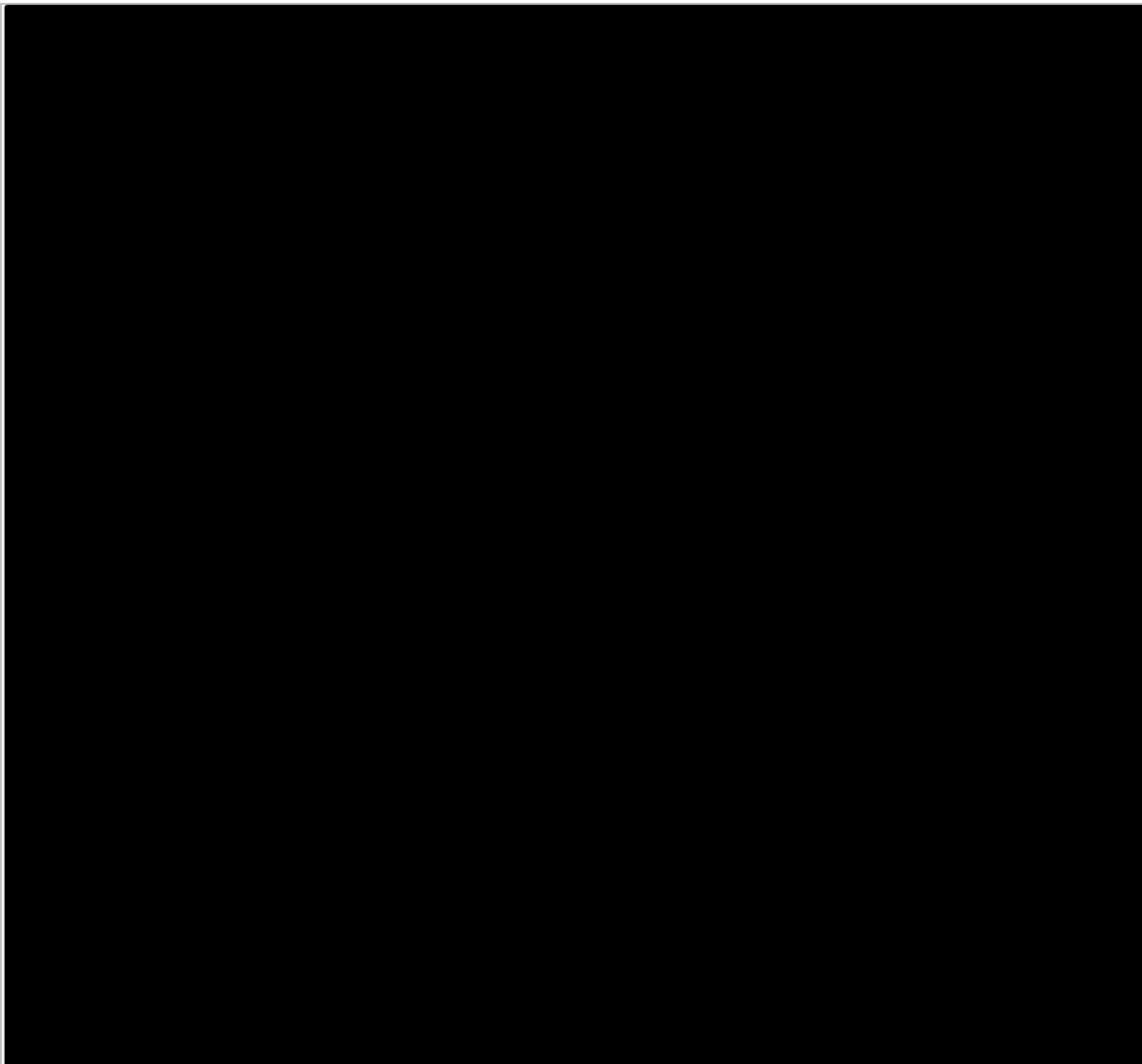
[Redacted text block]











I 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.

Q9 - Describe your approach to problem management and how you would contribute to identification and resolution of problems. Please feel free to include any diagrams/process flows into your answer – 10%





Crown
Commercial
Service



[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]



[Redacted text block]

J 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.

Q10 – Describe your approach to request management and how you ensure these are monitored and managed to achieve customer satisfaction. Please feel free to include any diagrams/process flows into your answer – 10%

[Redacted text block]



[Redacted content]



[Redacted]

[Redacted]

K 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

Q11 – Describe your approach to configuration management and how you would contribute to identification and updates of configuration items and dependencies. Please feel free to include any diagrams/process flows into your answer – 5%

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]



[Redacted content]



[Redacted content]

L 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

Q12 – Describe your approach to the analysis of customer satisfaction feedback, and how you would use these findings to improve service quality – 5%

[Redacted content]



[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]



Q13 - 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.

Yes

Yes

Describe your approach to delivery of the required Cloud Services Lifecycle Management services in a pandemic lockdown scenario – 5%

Q16 – Explain how you will manage, monitor and achieve the expected performance criteria specified in the FSA SLA document – 5%



The image shows a document that has been almost entirely redacted with thick black horizontal bars. The redaction covers the majority of the text area. On the left side, there are several small blue dots, which appear to be markers for a table of contents or a list of items. The dots are positioned at the start of several lines of text that are otherwise obscured by the redaction bars. The overall layout suggests a structured document, possibly a report or a list, where the specific details have been removed for security or privacy reasons.

[illegible]

[illegible]

Section 2: Ways of Working – 15%



- **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**

Q17 - Describe your experience of working with a range of different suppliers and how you are able to integrate successfully with them – 20%

[Redacted content]

- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Q18 - Describe your approach to complex or major incident management in a disaggregated service delivery model – 20%

[Redacted]



[Redacted content]



[Redacted text block]

- [Redacted text]
- [Redacted text]

[Redacted text block]

[Redacted text block]

[Large redacted text block]

- [Redacted text]

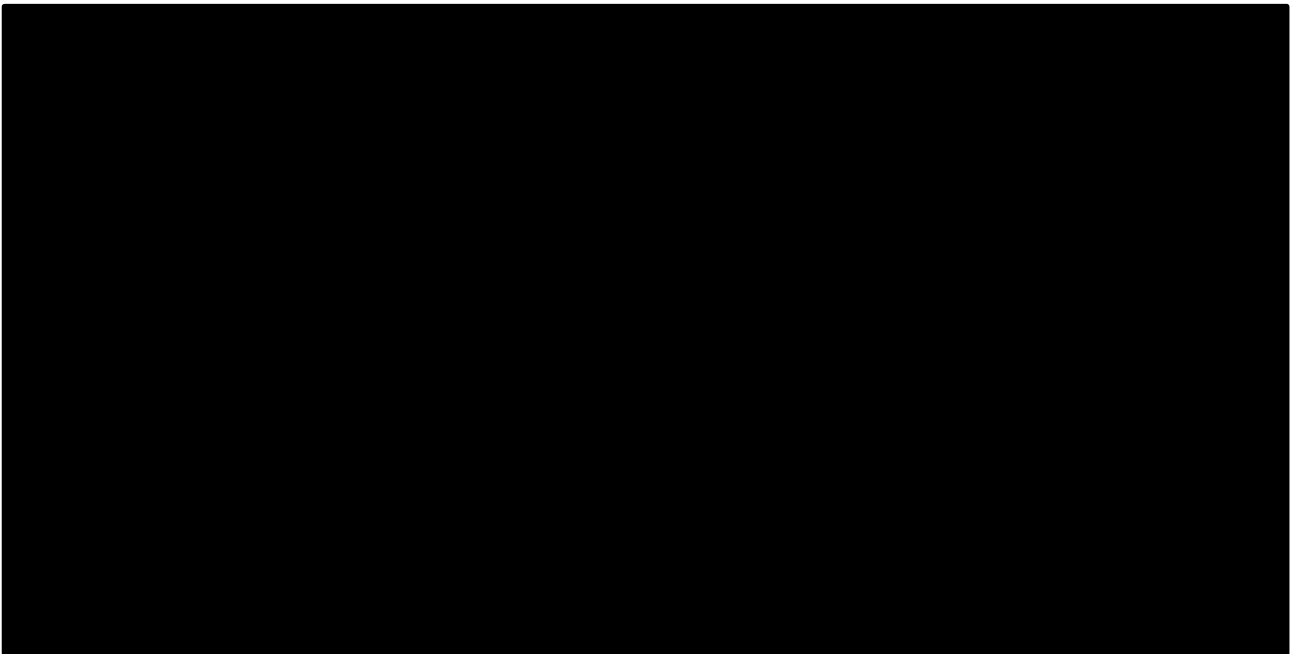
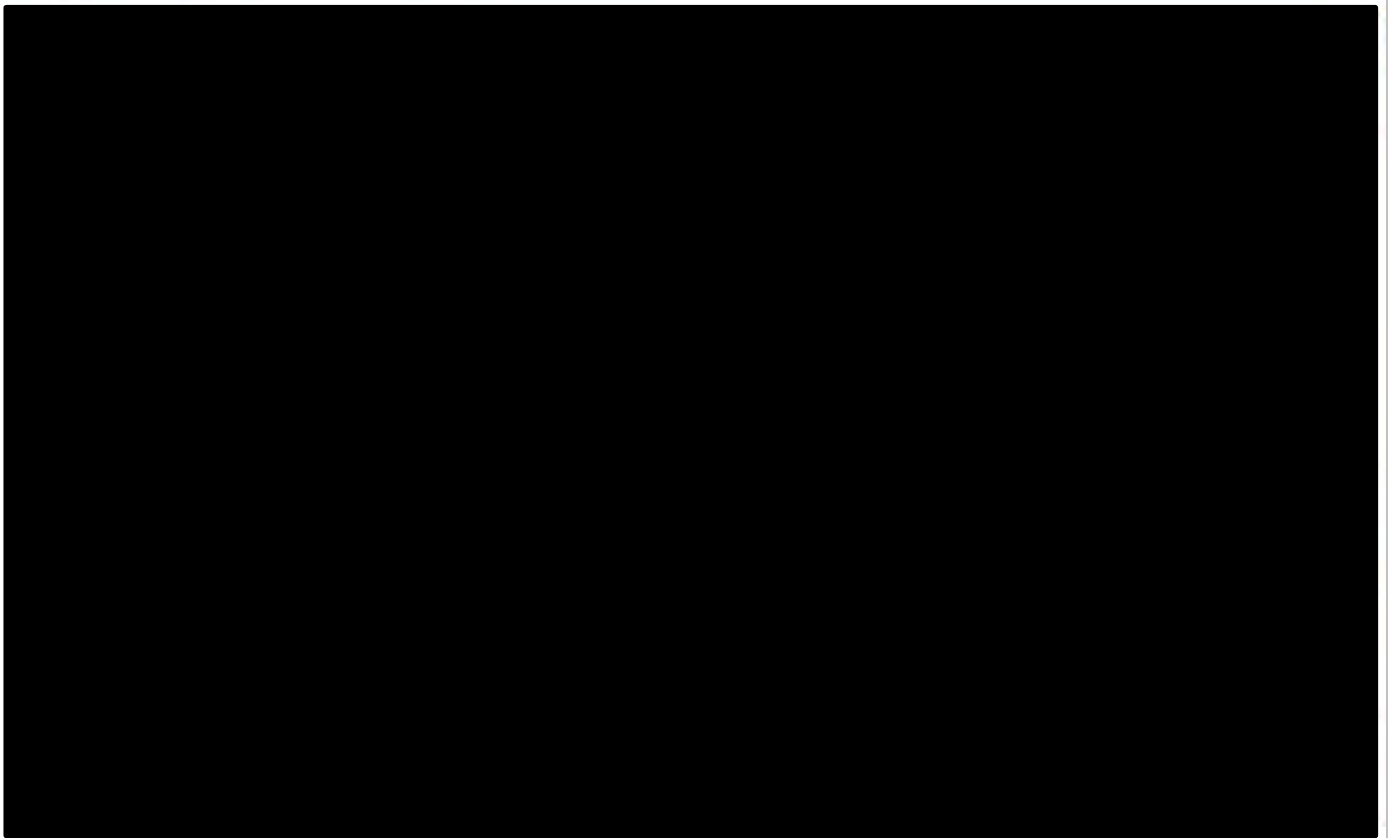
[Redacted text block]

- [Redacted text]
- [Redacted text]
- [Redacted text]

[Redacted text block]

[Redacted text block]

[Redacted text block]





[Redacted text block]

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

Q19 - Describe your approach to testing for new services related to Cloud Service Lifecycle Management that you use and / or support– 15%

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted content]

C ITIL Principles - ITIL principles must be followed

Q20 - Describe how you ensure your staff have an appropriate understanding of ITIL principles – 1%

[Redacted content]



[Redacted text block]

Q21 - Describe how you will ensure your staff members adopt and understand FSA's policies and procedures – 14%

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[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.

Q22 – Explain how you plan to resource this service offering, detailing key personnel and escalation routes– 20%

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



The diagram consists of a series of black rectangular blocks of varying sizes, arranged in a hierarchical or flow-like structure. On the left side, there are several small blue dots, some of which are aligned with specific blocks, possibly indicating a sequence or a specific point of interest. The blocks are connected by thin lines, creating a network-like structure. The overall layout suggests a complex system or process being analyzed or represented.



[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

Q23 - Describe how you will ensure the services you provide are consistent with FSA technology stack and Evergreen principles – 10%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[illegible]



[Redacted content]



Figure 1 displays a 3D visualization of the 1000 random samples of the posterior distribution of the parameters of the model. The plot shows three axes: α (ranging from 0 to 1), β (ranging from 0 to 1), and γ (ranging from 0 to 1). The distribution is concentrated in the region where α is high (near 1) and β and γ are low (near 0).

Section 3: Project Management – 5%



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.

Q24 – 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.

Q25 – Please confirm that you are able to provide this - Yes/No response – 50%

Yes

Section 4: Security Management – Personnel Security – 10%

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.

Q26 – 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

Q27 - 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

Q28 – 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 5: Security Management - Compliance – 15%

A Compliance

Q29 - 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 – 10%

Yes

Q30 - The Supplier will comply with the FSA access policy for access to FSA Systems/Services

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

Yes

Q31 – The supplier will implement self-service password reset.

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

Yes

Q32 – The FSA receives a monthly threat surface report and the supplier will undertake to resolve any vulnerabilities and issues this identifies in the service for which they are responsible.

Please confirm you agree to this – Yes/No response – 15%

Yes

Q33 - The retention periods for audit records and event logs will be agreed with the FSA and documented.

Please confirm you agree to this – Yes/No response – 15%

Yes

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

Q34 - Can you describe how you would deliver a zero trust approach to Office365 which includes Multi Factor Authentication and conditional access policies to ensure users are authenticated and presented



with a MFA challenge when this falls outside permitted routes. Can you please provide an example case study – 10%

[REDACTED]

- [REDACTED]
- [REDACTED]

- [REDACTED]

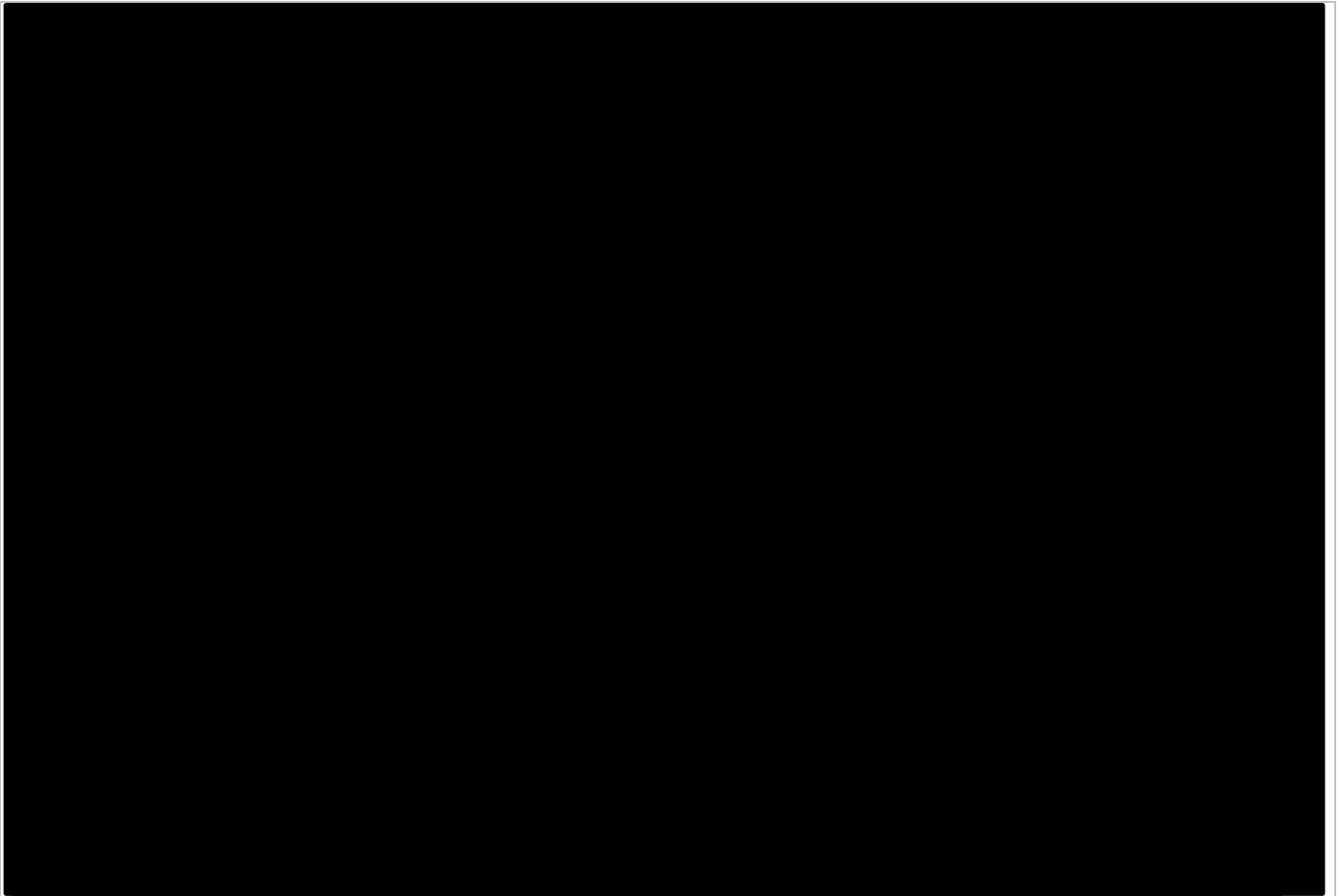
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]
- [Redacted text]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted]

C 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.

Q35 - How would you present monitoring data to show compliance and trend analysis which can be readily shared to the FSA Board and business community – 30%

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

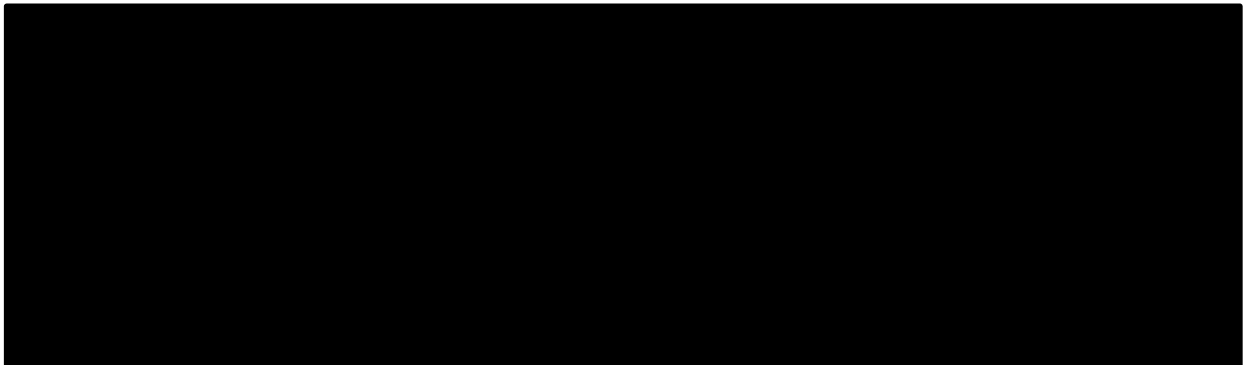
[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]



Section 6: Security Management - Vulnerabilities and Patching – 8%

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.

Q36 - 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.

Please confirm you accept this – Yes/No response – 10%

Yes

Q37 - 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.

Please confirm you agree to this - Yes/No response – 15%

Yes

Q38 - 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 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 on approval from the FSA.

Please confirm you agree to this - Yes/No response – 15%

Yes

Q39 - The Supplier will provide documented evidence to demonstrate the provisions for major version upgrades of the service, and is responsible to ensure the Service is always in mainstream support and complies with FSA patching policy of n-1 unless otherwise agreed by the FSA in writing.



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

Yes

Q40 - The Supplier will regularly test for the presence of known vulnerabilities and common configuration errors

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

Yes

B The Supplier 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

Q41 - 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 content]

- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]
- [Redacted content]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted text block]
- [Redacted text block]
- [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted text block]
- [Redacted text block]
- [Redacted text block]
- [Redacted text block]
- [Redacted text block]



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

• [Redacted]

[Redacted]

• [Redacted]



<div></div>
Section 7: 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
Q42 - Please confirm - Yes/No response – 100%
Yes
Section 8: Security Testing: IT Health Check – 1%
A The Supplier will co-operate with the FSA annual IT Health Check and project specific tests by a CHECK IT supplier and be responsible for implementing any actions assigned to them in the resulting remedial action plan
Q43 - Please confirm you agree to this - Yes/No response – 100%
Yes
Section 9: Security – Assurance – 3%
A Assurance
Q44 - The Supplier will provide copies of their data protection security patching, protective monitoring, access and security policies to the FSA.
Please confirm you agree to this - Yes/No response – 10%
Yes
Q45 - The Supplier will work with the FSA to complete a Personal Data Processing Statement as part of the contract
Please confirm you agree to this - Yes/No response – 20%
Yes
Q46 - The Supplier will work with the FSA to mitigate any risks assigned to them in the Privacy Impact Assessment if applicable.
Please confirm you agree to this - Yes/No response – 10%



Yes

Q47 - 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 confirm you agree to this - Yes/No response – 20%

Yes

B The Supplier will implement the records management policies of the FSA into M365

Q48- Can you please describe how you would configure M365 to meet the FSA's retention schedules – 40%

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Section 10: Security – Compliance Audits – 2%

A Compliance Audits


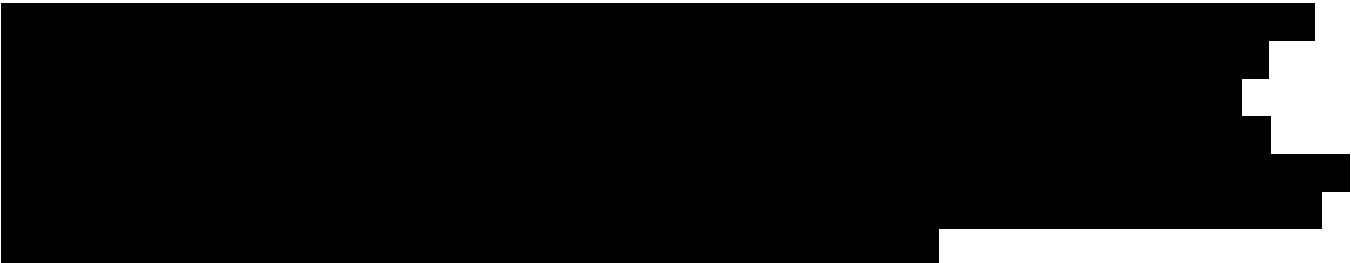
Q49 - The Supplier will support compliance with security assurance audit activity carried out by FSA against these requirements see link <https://www.gov.uk/government/publications/government-supplier-assurance-framework>.

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

Yes



Commercial ITT Response

8.15	TENDER	8.16	FS430634 – Cloud Service Management
Section 1: On-boarding Cost – 10%			
A To demonstrate that the supplier has a full understanding of any potential onboarding costs.			
Q1 – Please provide a breakdown of onboarding costs that your organisation anticipates – 100%			
Please complete the On-boarding Commercial Template.			
Completed			
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%			
Please complete the Initial Fixed Monthly Cost Commercial Template.			
completed			
Section 3: Flexible Charging – Decrease – 4%			
8.24	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.		
8.25	Q3 - How you would adjust the fixed monthly cost following a reduction in the number of applications across the tenancy (in particular in SharePoint or Power Platform) and what are the thresholds for triggering cost reductions.– 100%		
8.26			
			



[Redacted]

[Redacted]

[Redacted]

Section 4: Flexible Charging – Increase – 6%

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 - How you would adjust the fixed monthly cost following an increase in the number of applications across the tenancy (in particular in SharePoint or Power Platform) and what are the thresholds for triggering a cost increase – 100%

[Redacted]

[Redacted]



[Redacted]

- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Section 5: Change Management – 4%

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 – 100%

[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]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

A stylized illustration of a person with long, dark, wavy hair and a blue headband, looking down at a large, open book. The book has a blue cover and a white page with a blue border. The background is a light blue gradient.

[illegible]



[Redacted content]



[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

Section 7: 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%

[Redacted]



Post Tender Clarifications

POST TENDER CLARIFICATIONS

PROJECT REFERENCE : FS430634

PROJECT TITLE : Cloud Service Management

Date : 26 July 2021

9 Between: The Food Standards Agency (the Authority) and Methods Business and Digital Technology (the Contractor)

1. The Tender is revised as follows:

Clarification 1:

Requirement	Query	Action required	Methods Answer
Service Section E Question 5: Describe how you produce design documentation and how you ensure that documents are accurate and up-to-date. Please provide examples of design documentation content/format	The question is answered but there is no reference to adding this documentation to the knowledge base, there is reference to teams or a 'hub' owned by Core Azure.	Confirm that the document will be added to the knowledge management area in FSAs instance of Service Now by the supplier once it has been reviewed and approved by all parties.	We can confirm that the document will be added to the knowledge management area in FSAs instance of Service Now once it has been reviewed and approved by all parties.
Operational Section 2 Question 10: Describe your experience of managing the Windows Active Directory architecture (domains, sites, subnets) for a customer similar to FSA. Please make particular reference to how you ensured that domain controllers and the AD Function Level were upgraded to maintain currency with Windows Server releases	The question has been answered but FSA were looking for specific examples of how Core Azure would approach upgrades to the latest versions.	Confirm what the mechanisms are for triggering the upgrades and what the process is for keeping enterprise applications in line with the latest version/releases.	The mechanism for triggering upgrades and for keeping enterprise apps in line with the latest version/releases is set out in our response to Q41 in Service Requirements e.g. we will utilise the FSA's CMDB to prioritise the application of patches, and updates in order to validate that the estate complies with the N-1 policy.
Commercial Section 2 Question 2: Using the metrics supplied, you are required to	Assumptions row 28: There is a list of projects not included in the fixed monthly costs.	Our understanding was that the fixed monthly cost was made up of BAU	Yes, we can confirm that the projects listed under assumptions (row 28) can be



provide your initial monthly fixed price costs		support/maintain activity and a pot of project funding. Confirm that the projects listed can be drawn off that monthly project fund.	drawn off via the monthly project fund.
Commercial Section 3 Question 3: How you would adjust the fixed monthly cost following a reduction in the number of applications across the tenancy (in particular in SharePoint or Power Platform) and what are the thresholds for triggering cost reductions.	Question answered but example provided triggered some follow up questions.	Confirm how the capped incidents totals were calculated and what the definitions are for each of the incident categories (i.e. security incidents?)	The metrics chosen were used to demonstrate how we would adjust the fixed monthly cost e.g. the metrics are more reflective of the effort impact of reducing the number of applications across the tenancy. The metrics proposed are based on the information provided by the FSA.

Response (if required):

- 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.
- 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.
- 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

Signature:

[Redacted Signature]

Name:

[Redacted Name]

Title:

[Redacted Title]

For the Contractor

Signature:

[Redacted Signature]

Name:

[Redacted Name]

Title:

[Redacted Title]



Crown
Commercial
Service

Date:

Date: