Crown Commercial Service

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

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 16/06/2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1234. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

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

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

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Schedule of Processing, Personal Data and Data Subjects;
9. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

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

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

.1.2 the Order Form;

.1.3 the Call Off Terms; and

.1.4 Framework Schedule 18 (Tender).

Crown Commercial Service

Section A
General information

Contract Details	
Contract Reference:	C21608
Contract Title:	AWS Outbound Apps Transit and Internet Gateway
Contract Description:	Provision of a fully managed service for the hosting, configuration, and support of a new combined Internet Gateway / Egress and Apps Transit VPC within AWS in accordance with Attachment 1 Services Specification
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	£1,222,066.00
Estimated Year 1 Charges:	£461,749
Commencement Date: this should be the date of the last signature on Section E of this Order Form	Date of last signature of this Order Form

Buyer details

Buyer organisation name
Department for the Environment, Food and Rural Affairs (Defra)

Billing address
Your organisation's billing address - please ensure you include a postcode
Accounts Payable (Defra), SSCL, PO Box 797, Newport, Gwent, NP10 8FZ

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

Buyer representative contact details
Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
Quay House | 2 East Station Road | Peterborough | PE2 8YY
[redacted]

Buyer Project Reference
Please provide the customer project reference number.
P-31138

Crown Commercial Service

Supplier details

Supplier name
The supplier organisation name, as it appears in the Framework Agreement
Atos IT Services UK Ltd

Supplier address
Supplier's registered address
Second Floor MidCity Place,
71 High Holborn,
London, UK
WC1V 6EA

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. This must include an email for the purpose of Clause 50.6 of the Contract.
[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.
C21608

Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name
The guarantor organisation name

Not Applicable

Guarantor Company Number
Guarantor's registered company number

Not Applicable

Guarantor Registered Address
Guarantor's registered address

Not Applicable

Crown Commercial Service

Section B
Part A – Framework Lot

Framework Lot under which this Order is being placed
Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

1.	TECHNOLOGY STRATEGY & SERVICES DESIGN	☑
2.	TRANSITION & TRANSFORMATION	☑
3.	OPERATIONAL SERVICES	
	a: End User Services	☑
	b: Operational Management	☑
	c: Technical Management	☑
	d: Application and Data Management	☐
5.	SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period
Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months
36 months from service start date

Extension Period (Optional) Months
24 (2 x 12)

Minimum Notice Period for exercise of Termination Without Cause 90 days
(Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Sites for the provision of the Services

Crown Commercial Service

Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.

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

Not Applicable

Supplier Premises:

Not Applicable

Third Party Premises:

Not Applicable

Buyer Assets
Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms
Not Applicable

Additional Standards
Guidance *Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*

As defined in Attachment 1 Services Specification

Buyer Security Policy
Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

As defined in Attachment 1 Services Specification

Buyer ICT Policy
Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.

As defined in Attachment 1 Services Specification

Insurance
Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) - Not Applicable

Professional Indemnity Insurance (£) – Not Applicable

Buyer Responsibilities
Guidance Note: list any applicable Buyer Responsibilities below.

As defined in Attachment 1 Services Specification, paragraph 6 Buyer Responsibilities

Crown Commercial Service

Goods
Guidance Note: list any Goods and their prices.

Not Applicable

Governance – Option Part A or Part B
Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

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

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B
Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	X
Part B – Long Form Change Control Schedule	☐

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £[*insert details*]; and
- for the purpose of Paragraph 8.2.2, the figure shall be £[*insert details*].

Crown Commercial Service

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules
Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	X
S2: Testing Procedures	☐
S3: Security Requirements (either Part A or Part B)	Part B Applies
S4: Staff Transfer	☐
S5: Benchmarking	☐
S6: Business Continuity and Disaster Recovery	X
S7: Continuous Improvement	X
S8: Guarantee	☐
S9: MOD Terms	☐

Part B – Additional Clauses
Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	☐
C2: Security Measures	☐
C3: Collaboration Agreement	☐

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses
Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	☐
Northern Ireland Law	☐
Joint Controller Clauses	☐

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Crown Commercial Service

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)
Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

Not Applicable

Additional Schedule S4 (Staff Transfer)
Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Not Applicable

Additional Clause C1 (Relevant Convictions)
Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

Not Applicable

Additional Clause C3 (Collaboration Agreement)
Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not Applicable

Crown Commercial Service

Section D
Supplier Response

Commercially Sensitive information
Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Commercially Sensitive Information	**Period exemption is sought (Months)**
Any and all details of the Supplier's personnel and personal data (including Key Personnel and the personal data of the Supplier proposed contractors), including that: i) in any of the bid documents submitted by Supplier; and ii) in and/or related to the Call Off Contract.	Without limit
Service performance related material, including but not limited to: a) Regular and ad-hoc service reports to be produced under the Call Off Contract c) Rectification plans and material related to the conduct and/or outcome of such plans produced under the Call Off Contract d) Material disclosed in relation to audits undertaken in relation to the Call Off Contract, including that: i) in any of the bid documents submitted by Supplier; and ii) in and/or related to the Call Off Contract.	Term + 5 years
All details of the deliverables (including IPR and methodology and tools used, if any) set out in the Bidder's Response and software and other materials utilised by the Supplier as set out in the Response, including that: i) in any of the bid documents submitted by Supplier; and ii) in and/or related to the Call Off Contract.	Term + 5 years
Information and documents provided relating to the Supplier's insurance coverage and financial position provided in the Bidder's Response or under the Call Off Contract, including that: i) in any of the bid documents submitted by Supplier; and ii) in and/or related to the Call Off Contract.	Term + 5 years
Any document or section of a document containing pricing and invoicing information, including but not limited to estimates, evaluation reports and proposals provided under the Call Off Contract, including that: i) in any of the bid documents submitted by Supplier; and ii) in and/or related to the Call Off Contract.	Term + 5 years

Any information that relates the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Supplier and any other Information provided by the Supplier that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes to Buyer's attention or into the Buyer's possession.	Term + 5 years

Crown
Commercial
Service

Section E
Contract Award

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

SIGNATURES

For and on behalf of the Supplier

Name	[redacted]
Job role/title	[redacted]
Signature	[redacted]
Date	26 October 2023

For and on behalf of the Buyer

Name	[redacted]
Job role/title	[redacted]
Signature	[redacted]
Date	27th October 2023

Crown Commercial Service

Attachment 1 – Services Specification

1 BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

1.1 Defra's Cloud hosting is now the primary and preferred deployment for all Defra Group systems (wherever possible).

1.2 The architecture and design, particularly around internet access, needs to be consistent, secure, and robust. As part of this, access to the internet from Defra's cloud environments is a critical function for inbound and outbound access requirements.

1.3 Azure is already built with a managed 'Cloud DMZ' Outbound gateway and 'Apps Transit' vNet using Palo Alto firewall appliances which provide Azure servers and applications a secured path for external access to the internet.

1.3.1 The contract for that service expires on 1st January 2024.

1.4 This capability is lacking in AWS for any standardised or assured internet egress traffic and internal cloud controls between VPCs or from the internal Defra network.

1.4.1 Egress requirements are fulfilled by NAT gateways or gateway solutions which have been deployed on a case-by-case basis under LAP (DEFRA's Legacy Application Programme).

1.5 The Defra cloud environment in AWS therefore requires a project to implement a new 'local" Outbound Gateway with similar functionality & security to route AWS based resources externally as required for updates or internet service consumption (e.g. APIs).

1.6 The overall requirement is to build and manage a new strategic Outbound Apps Transit and Internet Gateway within Defra's AWS Cloud.

1.7 The AWS Outbound Apps Transit and Internet Gateway Solution will need to take into consideration alignment with the equivalent Azure service to provide a consistent technology across AWS and Azure.

1.8 As the strategic objective is to have a secure and robust solution in both AWS and Azure, any selected solution for AWS as part of this Further Competition Invitation should consider any future support and migration complexity in Azure due to vendor choice, management platforms, support locations, etc.

1.8.1 Modification to the service in Azure will be limited to amending/adding new rulesets only.

1.8.1.1 Note: This will be undertaken by the incumbent Provider.

1.8.2 Should there be a need for other modification/update to Azure in the future, this will be delivered under a new project.

1.8.3 At the time when the existing contract for the managed Cloud DMZ Outbound gateway and Apps Transit vNet in Azure expires, it is expected that any transition of the service and its support will be complete and covered under this contract.

1.8.4 The intention is for both solutions to be managed under a single contract and for the service to be co-termed.

2 Once the AWS Outbound Apps Transit and Internet Gateway has been established, migration of any/all existing tactical solutions will be arranged by the project team with the relevant Suppliers (using the CEDS PIR process) and/or internal DEFRA teams; along with any decommissioning activities required. **DEFINITIONS**

Expression or Acronym	Definition
API	Application programming interface
Apps Transit	Transit Gateway
ASA	Cisco Adaptive Security Appliance (ASA) firewall
AWS	Amazon Web Services, Cloud hosting platform
Azure	Microsoft Cloud hosting platform
BGP	Border Gateway Protocol
CCoE	DEFRA's Cloud Centre of Excellence
CEDS PIR process	Commercial Engagement and Delivery with Suppliers Project Initiation Request Process
DDTS	Defra's digital, data and technology service
DEFRA	Department for Environment, Food and Rural Affairs
DMZ	Network Demilitarized zone
MPLS Hub	Multi-Protocol Label Switching hub
NGFW	Next generation firewall
TGW	AWS Transit Gateway
UTM	Unified threat management
vNET	Virtual Network
VPC	Virtual Private Cloud

Crown Commercial Service

3 HIGH LEVEL SCOPE OF REQUIREMENT

3.1 Provide a fully managed service for the hosting, configuration, and support of a new combined Internet Gateway / Egress and Apps Transit VPC within AWS.

3.2 Migrate existing rules onto the new AWS Outbound Apps Transit and Internet Gateway firewalls to enable security and filtering of traffic to and from the internal Defra WAN.

3.3 Implement the required pattern to the new AWS Outbound Internet and Apps Transit Gateway.

3.4 Design, implement, and test the new AWS Outbound Apps Transit and Internet Gateway.

3.5 Design the solution to meet the requirements of a Tier 1 service, as defined in the DDTS Service Tiering Framework (see section 20 below).

3.6 Manage the service in accordance with the requirements of a Tier 1 service, as defined in the DDTS Service Tiering Framework (see section 20 below).

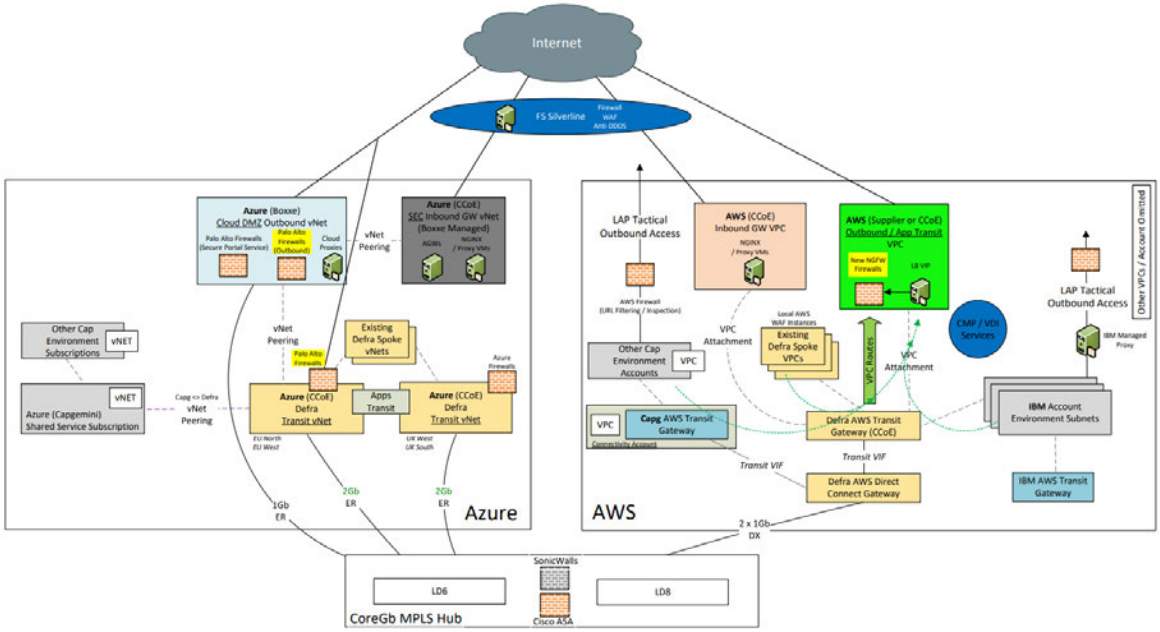
3.7 Provide a service model and commercial structure that allows for BAU changes to be made as part of the contract operating cost

3.7.1 Agreement is to be reached on the pricing structure for additional BAU changes to be made should the requirement exceed this value.

3.8 Enable the required access for Defra CCoE to view logs and make rule changes as part of the BAU service.

3.9 Anything not listed in this document is to be considered out of scope.

3.10 Intended end state:


Internet
FS Silverline
Azure (Boxxe)
Cloud DMZ Outbound vNet
Azure (CCoE)
SEC Inbound GW vNet
(Boxxe Managed)
vNet Peering
Other Cap Environment Subscriptions
vNET
Azure (Capgemini) Shared Service Subscription
Existing Defra Spoke vNets
Azure (CCoE) Defra Transit vNet
Apps Transit
Azure (CCoE) Defra Transit vNet
1Gb ER
2Gb ER
2Gb ER
Azure
LAP Tactical Outbound Access
AWS (CCoE) Inbound GW VPC
AWS (Supplier or CCoE) Outbound / App Transit VPC
VPC Attachment
Existing Defra Spoke VPCs
VPC Routes
CMP / VDI Services
LAP Tactical Outbound Access
Other VPCs / Account Omitted
Other Cap Environment Accounts
VPC
Capg AWS Transit Gateway
Defra AWS Transit Gateway (CCoE)
IBM Account Environment Subnets
Transit VIF
Defra AWS Direct Connect Gateway
IBM AWS Transit Gateway
AWS
2 x 1Gb DX
SonicWalls
LD6
LD8
CoreGb MPLS Hub
Cisco ASA

4 THE REQUIREMENT

4.1 FUNCTIONAL REQUIREMENTS

4.1.1 Provide a fully managed “Apps Transit” / Egress Gateway security service within the Defra AWS cloud environment to cover the following use cases:

4.1.1.1 Secure all AWS server and application egress access to the internet.

4.1.1.2 Provide South to North / North to South filtering of traffic between Defra AWS / internal WAN i.e., anything going to and from the MPLS Hub.

4.1.1.3 Provide horizontal filtering of traffic routing between VPCs within AWS.

4.1.1.4 Integrate with the TGW or AWS natively to support its function as the central secure transit hub.

4.1.2 AWS Outbound Apps Transit and Internet Gateway should secure:

4.1.2.1 all traffic to and from the internal Defra WAN to AWS cloud;

4.1.2.2 all traffic between VPCs in AWS cloud; and

4.1.2.3 all traffic that egresses to the internet from AWS hosted servers and applications.

4.1.3 The AWS Outbound Apps Transit and Internet Gateway service should be fully resilient and capable of throughput in excess of 10Gbps, both to the internet and between VPCs in AWS.

4.1.3.1 This throughput must be achievable once features have been enabled.

4.1.4 The appliances being introduced in AWS should have equivalent capacity to the current appliances used in Azure (Palo Alto VM-700).

4.1.5 The service should be scalable.

4.1.6 The AWS Outbound Apps Transit and Internet Gateway should be implemented in the EU-West-2 AWS region across 3 Availability Zones currently in use by Defra for cloud deployments.

4.1.7 The AWS Outbound Apps Transit and Internet Gateway must enable transparently forwarding to the internet via a default route; as well as present a load balancer / proxy VIP for services to that require a proxy target address.

4.1.8 The security policies must also include URL access policies to support end user access from VDI / Citrix based servers hosted within the cloud.

4.1.9 All traffic bound towards to the internet must be appropriately secured using NGFW appliances and provide the following features, as a minimum:

4.1.9.1 URL filtering;

4.1.9.2 SSL inspection;

4.1.9.3 AV/Anti-Malware;

4.1.9.4 Threat Prevention;

4.1.9.5 Threat Intelligence;

4.1.9.6 DNS Security/Proxying; and

4.1.9.7 File Type filtering.

4.1.10 The NGFW should be capable of supporting dynamic routing protocols, including BGP, to enable traffic interception within AWS cloud.

4.1.11 The existing firewall security ruleset and policies for internet access already implemented elsewhere will be analysed and replicated on the new AWS Outbound Apps Transit and Internet Gateway firewall cluster for consistency.

4.1.11.1 Note: The current estimate is that the below objects need to be set up on the new AWS firewalls:

4.1.11.1..1 Legacy to Cloud:

a) 360 inside>outside

b) 430 outside>inside

4.1.11.1..2 Firewall policies with 1,400 network objects in 265 network groups;

4.1.11.1..3 1,140 entries to build 150 service groups; and

4.1.11.1..4 approx. 2,700 routing entries both static and learn from routing protocol.

4.1.12 Traffic flows across AWS will need to be assessed in order to ensure appropriate access rules can be applied to allow traffic from VPC to VPC within AWS.

4.1.13 Support migration of any existing AWS hosted desktops / servers / services to use the new AWS Outbound Apps Transit and Internet Gateway for internet access.

4.2 SERVICE & SUPPORT

4.2.1 The AWS Outbound Apps Transit and Internet Gateway service must deliver all requirements of a Tier 1 service, as defined by the DDTS Service Tiering Framework (see section 20 below).

4.2.2 The Supplier must provide a service that will accommodate adaptations that can occur from changes to configuration, patches or upgrades.

4.2.3 The Supplier must provide and manage the firewall appliances to meet the following conditions (but not limited to):

4.2.3.1 the required technical/operational functionality;

4.2.3.2 the required technical compatibility;

4.2.3.3 the required technical interoperability;

4.2.3.4 the vendors recommended version;

4.2.3.5 patched to vendors recommended security version.

4.2.4 The AWS Outbound Apps Transit and Internet Gateway service must provide delegated access to Defra CCoE for both read-only and write permissions to perform routine changes such as URL rule updates.

4.2.5 Changes to the AWS Outbound Apps Transit and Internet Gateway service must be aligned to MyIT / ServiceNow ticketing and governance processes.

4.2.5.1 Note: the option to utilise Defra's Jira instance for routine changes is to be agreed.

4.2.6 The Supplier must collaborate with the DDTS SOC, DDTS service designers, and other required DDTS teams to enable creation of required Service Design documentation for the AWS Outbound Apps Transit and Internet Gateway service.

4.2.7 The Supplier must provide a process for staged release of all updates, policy changes and/or patches.

4.2.8 The AWS Outbound Apps Transit and Internet Gateway service must adopt centralised management, change orchestration, reporting and logging:

4.2.8.1 integration of logs into the DEFRA Solar Winds solution for increased monitoring and control.

4.2.8.2 integration into any other monitoring/support tools and processes, including MyIT / ServiceNow ticketing and governance;

4.2.8.3 a logs feed in an agreed format to be ingested into Azure Sentinel, the enterprise SIEM tool used by the Defra SOC.

4.2.8.3. The content of the feed would be agreed at a security workshop.

4.2.9 System / Event logging must integrate with the Defra SIEM (Microsoft Sentinel) for visibility by Defra SOC.

4.2.9.1. Note: as a minimum the SOC would expect to receive where possible:

4.2.9.1..1 Geo IP location user or source IP, User ID, sign in and logout time (DTG).

4.2.9.1..2 Any system operational event / number that the user ID is carrying out (account failed to login, audit log being purged, system time being changed etc).

4.2.9.2 Note: The Defra SOC will define more detailed requirements during the design phase.

4.2.10 Enable Defra SolarWinds to poll and interface with the new AWS gateway devices to retrieve utilisation, device health etc. This will be separate to any supplier management or monitoring systems which should be applied as part of the delivering the service.

4.3 CHANGES

4.3.1 The Supplier is to supply a service model and commercial structure that allows for BAU changes to be made per annum as part of the contract operating cost.

4.3.1.1 It is estimated that 30 changes will occur per annum.

4.3.1.2 The current number of incidents per annum is approximately 24.

4.3.1.3 Maintenance changes such as those required as part of patching, maintenance and/or global security policy updates (but not limited to) are considered part of the BAU service management for the solution.

4.3.1.4 Changes that are required as part of projects or programmes are not considered to be BAU changes and will be costed on a case by case basis by the project team in question.

4.3.2 Unused changes should roll over to the next year of service covered under this contract.

4.3.3 The Supplier will share the pricing structure for additional changes to be made should the requirement exceed the values listed above.

4.4 DESIGN & IMPLEMENTATION

4.4.1 The design effort will include collaboration with Defra DDTS and CCoE to agree the technical approach required to integrate the new VPC into AWS.

4.4.2 Design requirements are to include:

4.4.2.1 An HLD document which will be presented to the Defra TDA for formal design governance / sign-off before further work on the project can commence.

4.4.2.2 An LLD, which should be made available the Authority; this will not be subject to formal governance.

4.5 GOVERNANCE

4.5.1 The Supplier must adhere to the Defra Service Management Operating Model (SMOM).

4.5.2 The Supplier must provide documentation for the management of the supported systems as specified in the SMOM.

4.5.3 The Supplier must provide an escalation process for any issues/concerns. e.g., poor service.

4.5.4 The Supplier must adhere to the Defra Service Management and Service Integration (SM&SI) operating model.

4.5.5 The Supplier must adhere to the Defra Major Incident Management (MIM) process.

4.5.5.1 The Supplier must provide a service that aligns with the current service level arrangement for P1, P2, P3 and P4 incidents.

4.5.6 The Supplier must adhere to the DDTS change management process.

4.5.6.1 Note: Supplier internal change management processes can also be followed in addition.

4.5.7 The Supplier must ensure delivery of the solution aligns with the Defra DDTS Service Delivery Lifecycle (SDLC) Framework.

4.5.8 The Supplier must adhere to the DDTS stage gate process for project delivery.

4.5.8.1 Note: Supplier internal project management delivery processes can also be followed in addition.

4.5.9 The Supplier will be required to attend internal Defra governance forums and meetings to provide input into architectural design meetings and decisions, where necessary.

4.5.10 The firewall ruleset, security inspection, and URL filtering policies to be applied to the new AWS Outbound Apps Transit and Internet Gateway must be presented to Defra Operational Security for review and sign off before implementation.

4.5.11 The AWS Outbound Apps Transit and Internet Gateway service must undergo a formal ITHC and complete Defra Security assurance prior to go-live.

4.6 SECURITY AND CONFIDENTIALITY REQUIREMENTS

4.6.1 The support shall provide a solution that complies with National Cyber Security Centre (NCSC) recommendations as outlined in the following link:

4.6.1.1 Cloud security guidance - NCSC.GOV.UK

4.6.2 Minimum level to achieve is Best:

4.6.2.1 https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

4.6.3 The solution must be tested via an independent 3rd party under the NCSC CHECK Scheme prior to go live and at agreed intervals throughout the life of the Service.

4.6.4 The Supplier must demonstrate any security certification (e.g., ISO27001) and provide independent certificates for validation.

4.6.4.1 Note: ISO 27001:2017 & ISO 27002:2017 certification is preferable; whilst ISO 27001:2013 is an absolute minimum.

4.6.4.2 Should the Supplier not have the most up to date Certification, details must be provided of plans to move to & get recertificated to ISO27001:2022 within three years' of the date of the contract award.

4.6.5 The Supplier must provide evidence of adherence to established best practice such as adherence to security controls recommended by OWASP, NIST, etc.

4.6.6 The Supplier must provide a security management plan referencing their security policies and procedures.

4.6.7 The Supplier must ensure that all staff with access to Authority information, data or systems are vetted to appropriate standards (minimum BPSS or national equivalent with elevated clearance levels for certain administrative role types to be agreed with the Authority).

4.6.8 The Supplier must provide notification of security incidents and breaches to Defra's security personnel and link into Defra's existing security monitoring and reporting tool set.

4.6.9 The Supplier must identify all third parties involved in the Supplier's service, detail the services they provide and provide evidence that they will meet the same security standards of the Supplier.

4.6.10 The Supplier must comply with the Defra Security Assurance process (process can be provided on request).

4.6.11 The Supplier must provide details of their internal incident management process relating to security incidents involving Authority information, data or systems.

4.6.12 The Supplier must provide details of their internal vulnerability management process relating to the systems processing or hosting Authority information as part of their service.

4.6.13 The Supplier must make the Authority aware of any significant changes to the service.

4.6.13.1 Such changes might include re-hosting, architectural changes, major code changes or changes to support arrangements.

4.6.14 The Supplier must provide details on how the service is segregated from other customers so that the Authority can determine whether the service is adequately protected.

4.6.15 The Supplier must provide details on how they will manage access control to ensure that access to Authority data is limited to only that required for administrative users to perform their roles.

4.6.16 The Supplier must ensure all access to the service by their staff will be logged and stored securely for an agreed period should analysis of this information be required.

4.6.17 The Supplier must provide evidence of management of the integrity of the service data, e.g., after a service outage.

4.6.18 The Supplier must provide evidence of monitoring for unusual activity and maintenance of records of events for future analysis and make available any logs and audit data relating to the service if required by the Authority.

4.6.19 The Supplier must confirm that passwords and account management capabilities of the Service meet the criteria set out in the Authority's Password Policy.

4.6.20 The Supplier must detail any international supply chains upon which the service is dependent, to include software, hardware and/or services.

4.6.21 The Supplier must confirm that data will only be stored and processed for its intended purpose and that the storage and processing will comply with relevant legislation.

4.6.22 The Supplier must confirm that system data will not be shared with any other party without prior approval and that only the minimum data will be shared to meet the approved needs.

4.6.23 The Supplier must confirm that the service will be capable of supporting data up to a maximum protective marking of **OFFICIAL- SENSITIVE**.

4.7 SERVICE LEVELS AND PERFORMANCE

4.7.1 Service requirements are as defined within the DDTS Service Tiering Framework.

4.7.2 The Authority will measure the quality of the Supplier's delivery and service by means compliance with the Non-Functional Requirements in the table below. Within 60 days of the Call-Off Commencement Date (or as otherwise agreed in writing) both Parties will work together in good faith to finalise and agree the performance measurement related with the applicable Service Levels set out in the table below, in accordance with the Change Control Procedure. Performance Reports against the agreed Service Levels will commence on the first month following agreement between the Parties of the above measurements and in line with the terms set out in Schedule 3 of the Call Off Terms.

Non-Functional Requirement (NFR)	Tier 1
Service hours	24 x 7
1st Line Service Desk	24 x 7
Referring Supplier Service Desk	24 x 7
Incident Management (IM)	24 x 7
Major Incident Management (MIM)	24 x 7
Availability as %	>=99.99%
Permitted unavailability in minutes (in a 28 day period)	4
Single points of failure	None
Locally resilient, i.e. more than one instance of the service	Yes
Geographically resilient	Yes
Recovery time objective (following complete service outage)	5 min – 4 hours

Recovery point objective (extent of data loss)	15 min – 1 hour
Disaster Recovery Test	Annually
Penetration test (off premise / externally facing)	Annually
Security patching	Monthly
Level of security monitoring & alerting	High
Level of vulnerability management	High
IT Service Management	
Service Governance	Monthly
Contract Review	Every 6 months

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

4.7.3 Glossary of service management terms above:

Term	Definition
Availability as a %	Availability is the amount of time the service is expected to be working during the agreed service hours (excluding any planned downtime).
Availability in minutes	This reflects the Availability % in terms of minutes over a 28 day period. In reality this number may differ where planned downtime is included in its calculation. The values shown here do not take planned downtime into account.
Contract review	How often the underpinning contracts that support the service are reviewed.
Disaster Recover test	How often the recovery plans to recover the service are tested.
Incident management	The process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.

Major incident management	The process responsible for managing the highest category of impact of incident that results in significant disruption to the business.
Penetration test	An authorised simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.
Permitted outage	Based on the availability % this is the number of allowable minutes downtime in a 28 day period
Recovery point objective (RPO)	The maximum amount of data that may be lost when service is restored after an interruption. The recovery point objective is expressed as a length of time before the failure. For example, a recovery point objective of one day may be supported by daily backups, and up to 24 hours of data may be lost. Recovery point objectives for each IT service should be negotiated, agreed and documented, and used as requirements for service design and IT service continuity plans.
Recovery time objective (RTO)	The maximum time allowed for the recovery of an IT service following an interruption. The service level to be provided may be less than normal service level targets. Recovery time objectives for each IT service should be negotiated, agreed and documented.
[Locally] resilient	The ability of an IT service or other configuration item to resist failure or to recover in a timely manner following a failure.
[Geographically] resilient	The same as Locally Resilient but resilience is configured across more than one physical location to deal with a localised environmental failure, e.g. a service configured across two data centres enabling the service to remain available in the event of a data centre failure.
[Level of] security monitoring & alerting	The level of auditing in place to monitor security events within the service.
Security patching	How regularly mandatory security patches are applied to the service as recommended by software manufacturers/distributors.
Service Governance	How often the performance of service is reviewed against agreed SLA's. It will track and review the performance of OLA's and underpinning contracts and continuous service improvement activities. Service Governance will be managed by the associated Service Owner.

Service hours	The time in the day when the service is expected to be available
[1st line] service desk	The hours of service of the Defra internal service desk, i.e. MyIT. It is the single point of contact between the service provider and the users, i.e. MyIT. The service desk manages incidents and service requests, and also handles communication with the users.
[Referring Supplier] service desk	The hours of the Supplier service desk where the Supplier has been contracted to provide additional support for the service. The service desk manages incidents and service requests referred to it by the 1st Line Service Desk.
Single points of failure	A single point of failure is a part of the service where should it fail will stop the service from being available.
[Level of] vulnerability management	The level of management of weaknesses that could be exploited by a threat. This is ensuring the right controls are in place and being implemented and managed effectively.

4.7.4 Termination in the event of a material default by the Supplier shall be in accordance with the RM6100 call-off terms.

4.8 CONTINUOUS IMPROVEMENT

4.8.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

4.8.2 The Supplier should present new ways of working to the Authority during monthly review meetings.

4.8.3 Attendance at review meetings shall be at the Supplier's own expense.

4.8.4 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

4.9 KEY MILESTONES AND DELIVERABLES

4.9.1 The following initial Contract milestones shall apply:

Milestone	Description	Timeframe or Delivery Date
1	Project kick off meeting	Within 2 weeks of the Expected commencement date for the Contract
2	Buyer to provide list of existing firewalls rules for AWS	Within 1 week of Project kick off meeting

3	First Service management meeting	Within 1 month of the Service going live

4.9.2 The Supplier must include a detailed description of their approach to supporting the service post go-live; taking in to account the requirements listed in section 4.7 above.

This should include details of service reporting / service reviews.

5 Risks

5.1 The following are the Risks identified against the implementation of the solution:

Risk	Mitigation
Negative impact on solution because of rule change executed by Defra CCoE Team on devices in-scope	Defra CCoE and the Supplier's teams will agree on a common operating model. The Supplier will work with Defra's Change Mgt Team to agree a suitable time period. Additionally, via a common CAB, both parties will be able to review changes to ensure alignment.
FortiGate devices being deployed into a live AWS environment which may cause disruptions to the Buyer's services	The Supplier will discuss change windows with the Buyer and create a plan for implementation of the new Gateway solution in order to achieve no disruption of service . The solution has been designed to be modular with 'avoidance of failure' and 'client-first' at the forefront—it can be easily scaled to meet traffic volumes, and it is the least intrusive solution (as to not interfere with enclaves managed by 3rd-parties).
Issues may arise when interfacing between solutions whilst working with other GSIs to integrate the proposed solution	As per the Project Plan, the Supplier will share the High-Level Design (HLD) document, and the Buyer will include the respective parties in the timely sign-off of this HLD. The Supplier has delivered numerous projects with multi-vendor solutions and we intend to bring our 'no blame'/'fix first' culture to the Buyer to ensure that any issues that arise do not become obstacles.

Risk	Mitigation
Fortinet is being introduced to the Defra environment as a new vendor and additional effort and governance may be required during implementation	The Supplier will leverage existing experience in delivering successful Fortinet deployments, utilizing out vast knowledge share bank as well as our certified Fortinet engineers and access to vendor resources, through our platinum partnerships. This relationship and support from Fortinet will include consultancy to help address any issues encountered which are specific to Defra's environment. Fortinet and AWS have a strong relationship themselves, and the technologies integrate easily—it's estimated that 100-200 UK customers deploy 1-10 firewalls, and there are tens of thousands globally.
Lack of visibility to all Defra requirements and cloud architecture, there is a possibility that solution may need to be revisited and re-costed at a later stage	The Supplier will use the Scoping & Discovery phase to finalise the HLD, detailing Defra's environment, with a timely-sign off by the Buyer's teams and GSIs. The Supplier will leverage its existing relationship with the CCoE team alongside its partnership relationship with AWS and Fortinet to validate the solution against Defra's AWS policies and environments.
Size and complexity of Current Mode of Operation (CMO) security policies is unknown, e.g. internet IDS/IPS can exceed Atos estimation, which is based on limited info provided by the Buyer	The Supplier will use the Scoping & Discovery phase to finalise the HLD, detailing Defra's environment, with a timely-sign off by Defra teams and GSIs. The Supplier will review the CMO security policies to understand if they are fit for purpose, and identifying efficiencies where appropriate to reduce complexity.

6 Buyer Responsibilities

6.1 The following are the dependencies of Supplier on the Buyer and its other 3rd-Parties (collectively referred to as "Buyer Responsibilities") In alignment with the timelines in the agreed Implementation Plan, the Buyer shall:

6.1.1 provide access to the Buyer's ServiceNow to the Supplier teams for incident management.

6.1.2 Create and share an updated list of the CCoE team to the Supplier to provide for both read-only and write permissions to perform routine changes such as URL rule updates

6.1.3 Renew and maintain software licenses for AWS environment

6.1.4 Provide the required access and authority to the Supplier's team to deploy and configure the required resources, including virtual machines, within the Buyer's AWS environment

6.1.5 Configure all required firewalls rules and ACI contracts on network devices not managed by the Supplier

6.1.6 Supply the firewall rules within 5 Working Days following the Project kick-off meeting

6.1.7 Provide access to the Defra AWS account tenancy to enable the Supplier's activities in the agreed Implementation Plan, at no cost to the Supplier.

7 Social Value Commitments

7.1 Fighting Climate Change

7.1.1 The Supplier will deliver additional environmental benefits in the performance of the contract, including working towards net zero greenhouse gas emissions, through the following commitments:

7.1.1.1 The Supplier will help the Buyer understand its carbon footprint across delivery and adopt sustainable delivery practices aligned to minimising emissions.

7.1.1.2 The Supplier will minimise workforce emissions and directly influence the carbon footprint of the contract workforce.

7.1.1.3 The Supplier will promote environmental awareness including promoting events by the Supplier's Green Network and organising joint initiatives with the Buyer. The Supplier will also identify knowledge sharing opportunities on the topic of sustainability.

7.1.2 The above commitments will be measured via the Supplier's social value measurement tool using the following metric(s):

- No. of people hours protecting/improving the environment.

7.2 Wellbeing

7.2.1 The Supplier will demonstrate action to support health and wellbeing, including physical and mental health, in the contract workforce, through the following commitments:

7.2.1.1 The Supplier will fund training for a member of the Supplier's workforce to become a Mental Health First Aider and be the dedicated support for Mental Health for this contract.

7.2.1.2 The Supplier will embed best practice ways of working into the delivery approach and agree this with the Buyer to support the wellbeing of the contract workforce.

7.2.1.3 The Supplier will engage and support the contract workforce to identify areas of continuous improvement related to health and wellbeing through feedback forums.

7.2.1.4 The Supplier will co-deliver a joint volunteering initiative each year with the Buyer and supply chain partners to support a community initiative aligned to the Buyer's values.

7.2.1.5 The Supplier will connect the Buyer with the Supplier's VCSE partners to increase understanding of the needs across different demographics in the community and embed lessons learnt into the co-design and delivery of the contract.

7.2.1.6 The Supplier will promote environmental awareness in the community through awareness campaigns and events, aligning with the Buyer's key priority to positively impact the environment for future generations.

7.2.2 The above commitments will be measured via the Supplier's social value measurement tool using the following metric(s):

- No. of implemented measures to improve the physical and mental health and wellbeing of employees across all companies in the supply chain under the contract

- No. of people hours spent supporting local community integration, such as volunteering and other community-led initiatives, under the contract.

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

#	Milestone Description	Milestone Payment amount (£GBP)	Milestone Date	Delay Payments (where Milestone) (£GBP per day)
M1	*N/A*	*N/A*	*N/A*	*N/A*
M2				
M3				
M4				
M5				

Part B – Service Charges

Upon completion of the Implementation Plan, Services will be charged on a Fixed Price basis for the following period in accordance with the following Monthly Service Charges during the Initial Term:

Charge Number	Service Charges	Frequency
Fixed Price Service Charges		
Service Charge	[redacted]	Monthly
Pen Test	[redacted]	Annual – single charge payable once incurred

All Charges are exclusive of VAT or any applicable tax.
The above Service Charges shall be subject to indexation from 1 April 2025 and shall be calculated in accordance with paragraph 3, Part C of Call Off Terms Schedule 2 Charges and Invoicing.

The above Monthly Service Charges are based upon the Buyer requirements stated in Paragraph 4.3 Changes of Attachment 1 – Services Specification which cover the following:

- Up to 30 x changes per annum (prorated for the first Contract Year)
- Up to 24 x incidents per annum (prorated for the first Contract Year)
- Support for 6 firewalls & 1 Gateway Load Balancer in 1 region across 3 Availability zones and FortiManager.
- Engineering time for joint CAB reviews

Any additional requirements not included in the above shall be charged separately on a Time and Material basis.

In accordance with Paragraph 4.3 Changes of Attachment 1 – Services Specification, Changes that are required as part of projects or programmes are not considered to be BAU changes and will be estimated on a case-by-case basis by the project team in question and will be agreed with the Buyer prior to implementation.

Should the maximum number of per annum changes and incidents not be fully utilised within the Contract Year, the Supplier shall increase the maximum number for the following Contract Year by a corresponding amount. Any remaining unutilised changes or incidents at contract expiry or termination shall not be refunded.

Estimated Basic Monthly Service Charges - Optional Extension Period

An Estimated Basic Service Charges for the optional Extension Period are outlined below subject to the followings:

- 3rd Party Charges such as Fortinet software tooling are not yet included in the estimate as quotes will have to be obtained closer to the time and will be added to below amount
- Assessment of volumes in scope. The ultimate charges may vary depending on the then volumes;
- Indexation will apply on the charges;

Charge Number	Estimated Basic Monthly Service Charges during Optional Extension	
Year 4	[redacted]	
Year 5	[redacted]	

All Charges are exclusive of VAT or any applicable tax.

The Parties shall agree the applicable Charges for the Optional Extension Period in accordance with the Change Control Process.

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

Supplier Personnel Rate Card

The following Supplier Personnel Rate Card for daily rates shall be used to calculate the relevant Charges where a Time and Materials pricing mechanism applies:

Crown
Commercial
Service

All Charges are exclusive of VAT or any applicable tax.

- Reimbursable Expenses shall be recovered by Supplier at cost and charged in accordance with paragraph 3, Part A of Call Off Terms Schedule 2 Charges and Invoicing.

- The above Supplier Personnel Rate Card shall be subject to indexation from 1 April 2025 and shall be calculated in accordance with paragraph 3, Part C of Call Off Terms Schedule 2 Charges and Invoicing.

Implementation Charges

- Charges for the delivery of the Implementation Plan and associated Milestones (the "Implementation Charges") shall be calculated on a Time and Materials basis.

- An initial estimate of the Implementation Charges is provided in the table below.

- The estimated Charges below are based on the known resource profile at the Commencement Date. Upon agreement by the Parties of the Implementation Plan, the Supplier shall review the estimated Charges and the Parties shall agree any variation to the estimated Charges in accordance with the Change Control Procedure.

Lot 1 (Technology Strategy and Services Design) and Lot 2 (Transition and Transformation)

TYPE OF COST	Role / Activity	SFIA Role	Day Rate	Days	Price
Own Staff	Engineer	[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]
[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]

Crown Commercial Service

Own Staff	[redacted]
Own Staff	[redacted]
Software Tooling	[redacted]
Software Tooling	[redacted]
Software Tooling	[redacted]
Subcon-tracted Services	[redacted]
	[redacted]
TOTAL	[redacted]

All Charges are exclusive of VAT or any applicable tax.

Fortinet costs converted from USD at the then current exchange rates of October 2023.

Reimbursable Expenses shall be recovered at cost and charged in accordance with paragraph 3, Part A of Call Off Terms Schedule 2 Charges and Invoicing.

The resource profile in the estimated Charges may flex where necessary to accommodate Buyer needs. Any such changes shall be agreed between the Parties and managed through the operational delivery governance and agreed at the monthly AWS Gateway Project Governance Board Meeting. The Supplier will charge the Buyer for actual staff utilisation during Implementation. The blend of SFIA skills within the team can be changed by agreement, in advance, with the Buyer.

The Supplier will charge third party costs at the point they are incurred.

Terms of use of all 3rd Party products or services are subject to the provider's standard terms and conditions.

The estimated Charges in the table above are subject to the following Risks, Assumptions and Dependencies.

Risks

Implementation Risks are outlined in Paragraph 5 of Attachment 1 – Services Specification. If any of these risks progress into issues, following implementation of agreed mitigations, and the Parties assess that there may or will be an impact on the time, quality and/or cost of the Implementation, the

Crown Commercial Service

Parties will work collaboratively to agree a suitable remediation which will be implemented in accordance with the Change Control Procedure.

Assumptions

Implementation Charges are adopted based on the following assumptions:

- The Buyer shall bear all costs associated with the AWS Platform;
- The Buyer shall bear any costs associated with other 3rd Parties providers unless expressly included in the Supplier Charges;

Dependencies

Implementation dependencies are outlined as Buyer Responsibilities in Paragraph 6 of Attachment 1 – Services Specification. If any of these dependencies have not been met in accordance with the agreed Implementation Plan, and the Parties assess that there may or will be an impact on the time, quality and/or cost of the Implementation, then the Parties will work collaboratively to agree a suitable remediation which will be implemented in accordance with the Change Control Procedure.

Crown Commercial Service

Implementation Plan

Notwithstanding Clause 3.1 of Additional clauses and Schedule, Buyer and Supplier agree that they will within 20 Working Days after the Commencement Date (or as otherwise agreed in writing) discuss and work out an agreed Detailed Implementation Plan.

Crown Commercial Service

Attachment 4 – Service Levels

Service Levels are defined in Attachment 1 Service Specification

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

.1.5 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

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

Part B – Key Sub-Contractors

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period	Key role in delivery of the Services
Eviden Technology Services LTD	registration number 146917 and registered address at 44 Esplanade, St Helier Jersey, JE4 9WG, acting through its UK establishment, Atos Holding UK 1 Limited, registered in England and Wales with UK establishment number BR025381	Technology Services	97%	YES

Crown Commercial Service

Attachment 6 – Software –

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

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

Part A – Supplier Software

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry

Crown Commercial Service

Part B – Third Party Software

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
[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]

Attachment 7 – Schedule of Processing, Personal Data and Data Subjects – Not Applicable No Personal Data is Processed

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: **[*Insert Contact details*]**
1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **[*Insert Contact details*]**
1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.
1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	**[The Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • ***[Insert the scope of Personal Data for which the purposes and means of the processing by the Supplier is determined by the Authority]*** **The Supplier is Controller and the Authority is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with Clause 34.2 to 34.15 of the following Personal Data: • ***[Insert the scope of Personal Data for which the purposes and means of the processing by the Authority is determined by the Supplier]*** **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: • ***[Insert the scope of Personal Data for which the purposes and means of the processing is determined by both Parties together]*** For the purpose of Clause 1.2 of the joint controller clauses the [insert either Buyer or Supplier] shall be the Party referenced and responsible for those matters set out in Clause 1.2(a)-(e). ***Insert for the purpose of Paragraph 1.2 of the joint controller clauses which Party (either Supplier or Buyer) shall be responsible for those matters listed in Clause 1.2(a) – (e), including whose privacy policy should apply i.e.*** **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:

	• ***Business contact details of Supplier Personnel,*** • ***Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under this Contract.*** • ***[Insert the scope of other Personal Data provided by one Party who is Data Controller to the other Party who will separately determine the nature and purposes of its processing the Personal Data on receipt.*** *e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer]*
Duration of the processing	***[Clearly set out the duration of the processing including dates]***
Nature and purposes of the processing	***[Please be as specific as possible, but make sure that you cover all intended purposes.*** ***The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.*** ***The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]***
Type of Personal Data	***[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]***
Categories of Data Subject	***[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]***
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	***[Describe how long the data will be retained for, how it be returned or destroyed]***

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

AWS Gateway Project governance Board (Implementation)	
Buyer Members for the Operational Board	Project Manager CCoE Representative Service Owner Other attendees as required
Supplier Members for the Operational Board	Delivery Manager Service Delivery Manager Other attendees as agreed with the Buyer
Frequency of the Operational Board	Monthly
Location of the Operational Board	Remote meeting unless otherwise agreed

Weekly Project Meeting (Implementation)	
Buyer Members for the Operational Board	Project Manager Other attendees as required
Supplier Members for the Operational Board	Delivery Manager Other attendees as agreed with the Buyer
Frequency of the Operational Board	Weekly
Location of the Operational Board	Remote meeting unless otherwise agreed

Service Meeting (BAU)	
Buyer Members for the Operational Board	Service Owner Defra Group Commercial Representative Other attendees as required
Supplier Members for the Operational Board	Service Delivery Manager Commercial Representative Other attendees as agreed with the Buyer
Frequency of the Operational Board	Monthly (unless otherwise agreed)
Location of the Operational Board	Remote meeting unless otherwise agreed

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

S1	Implementation Plan
S3	Security Requirements (Part B)
S6	Business Continuity and Disaster Recovery
S7	Continuous Improvement

Unless there is a clear adjustment to an existing provision of the Contract, additional Clauses incorporated into the Contract via the Order Form will have the effect of being inserted sequentially immediately after Clause 55. New definitions for Schedule 1 (Definitions) will have the effect of being inserted alphabetically into the table therein and associated schedules will have the effect of being inserted sequentially immediately after Schedule 10.

ADDITIONAL CLAUSES AND SCHEDULES - SCHEDULES

S1 IMPLEMENTATION PLAN

1. INTRODUCTION

1.1 This Schedule S1 (Implementation Plan):

1.1.1 defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and

1.1.2 identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2. OUTLINE IMPLEMENTATION PLAN

2.1 The Outline Implementation Plan is set out in Attachment 3 (outline Implementation Plan) the Order Form.

2.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause)).

3. APPROVAL OF THE DETAILED IMPLEMENTATION PLAN

3.1 The Supplier shall submit a draft of the Detailed Implementation Plan to the Buyer for approval within twenty (20) Working Days of the Commencement Date.

3.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

3.2.1 incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;

3.2.2 includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Milestones:

(a) the completion of each design document;

(b) the completion of the build phase;

(c) the completion of any Testing to be undertaken in accordance with Schedule S2 (Testing Procedures); and

(d) training and roll-out activities;

3.2.3 clearly outlines all the steps required to implement the Milestones to be achieved in the next 15 months (or such other period agreed between the Parties), together with a high level plan for the rest of the programme;

3.2.4 clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and

3.2.5 is produced using a software tool as specified, or agreed by the Buyer.

3.3 Prior to the submission of the draft Detailed Implementation Plan to the Buyer in accordance with Paragraph 3.1, the Buyer shall have the right:

3.3.1 to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:

(a) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;

(b) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and

(c) any other work in progress in relation to the Detailed Implementation Plan; and

3.3.2 to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Buyer shall:

3.4.1 review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and

3.4.2 notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than twenty (20) Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Buyer.

3.5 If the Buyer rejects the draft Detailed Implementation Plan:

3.5.1 the Buyer shall inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Buyer's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Buyer for the Buyer's approval within twenty (20) Working Days of the date of the Buyer's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3.6 If the Buyer approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Buyer’s notice of approval.

4. UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

4.1 Following the approval of the Detailed Implementation Plan by the Buyer:

4.1.1 the Supplier shall submit a revised Detailed Implementation Plan to the Buyer every three (3) months starting three (3) months from the Commencement Date;

4.1.2 without prejudice to Paragraph 4.1.1, the Buyer shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Buyer within twenty (20) Working Days of receiving such a request from the Buyer (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);

4.1.3 any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and

4.1.4 the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Service Management Board (as defined in Part B of Schedule 7 (Governance) where used) or any such service management board established under Part A of Schedule 7 (Governance) where used. In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Buyer not less than five (5) Working Days in advance of such meeting.

4.2 Save for any amendments which are of a type identified and notified by the Buyer (at the Buyer's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:

4.2.1 any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and

4.2.2 in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause).

4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Buyer.

5. GOVERNMENT REVIEWS

.1.3 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

S3 SECURITY REQUIREMENTS
PART B – LONG FORM SECURITY REQUIREMENTS

1. DEFINITIONS

1.1 In this Part B of Schedule S3 (Security Requirements), the following definitions shall apply:

"Baseline Security Requirements"	the baseline security requirements set out in Annex 1 of this Part B Schedule S3 (Security Requirements);
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Part B Schedule S3 (Security Requirements);
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Part B Schedule S3 (Security Requirements), a draft of which has been provided by the Supplier to the Buyer and is set out in the Order Form and as updated from time to time; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

.2

2. SECURITY REQUIREMENTS

2.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.2 The Parties shall each appoint a security representative to be responsible for security.

2.3 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.4 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Buyer Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Buyer Data remains under the effective control of the Supplier at all times.

2.6 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.7 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Commencement Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.7.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that:

3.3.1 if the Buyer has not stipulated that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Services and all processes associated with the provision of the associated with the delivery of the Services, including the Buyer Premises, the Sites,

the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 1.7;

3.5 at all times provide a level of security which:

3.5.1 is in accordance with the Law and this Contract;

3.5.2 complies with the Baseline Security Requirements;

3.5.3 as a minimum demonstrates Good Industry Practice;

3.5.4 complies with the Security Policy and the ICT Policy;

3.5.5 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework);

3.5.6 takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk);

3.5.7 complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

3.5.8 meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

3.5.9 addresses issues of incompatibility with the Supplier's own organisational security policies; and

3.5.10 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 3.12;

3.5.11 document the security incident management processes and incident response plans;

3.5.12 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.5.13 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.6 Subject to Paragraph 2, the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any

successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.7 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.8 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Part B Schedule S3 (Security Requirements). If the ISMS is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.7 shall be deemed to be reasonable.

3.9 Approval by the Buyer of the ISMS pursuant to Paragraph 1.3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Part B Schedule S3 (Security Requirements).

4. SECURITY MANAGEMENT PLAN

4.1 Within twenty (20) Working Days after the Commencement Date, the Supplier shall prepare and submit to the Buyer for approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in the Order Form;

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with Paragraph 3.5.4, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Part B Schedule S3 (Security Requirements) is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in

connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Part B Schedule S3 (Security Requirements) (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Services has minimised the Buyer and Supplier effort required to comply with this Part B Schedule S3 (Security Requirements) through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Commencement Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules of this Contract which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Part B Schedule S3 (Security Requirements).

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Part B Schedule S3 (Security Requirements). If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Part B Schedule S3 (Security Requirements).

5. AMENDMENT OF THE ISMS AND SECURITY MANAGEMENT PLAN

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Services and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with Paragraph 3.5.4, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to the Baseline Security Requirements or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. SECURITY TESTING

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary

in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or Baseline Security Requirements or the requirements of this Part B Schedule S3 (Security Requirements), the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. COMPLYING WITH THE ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with Paragraph [ ].

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph 7.1, the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. SECURITY BREACH

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

8.2.2 minimise the extent of actual or potential harm caused by any Breach of Security;

8.2.3 remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

8.2.4 apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Services so as to meet the relevant Service Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

8.2.5 prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

8.2.6 supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

8.2.7 as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Part B Schedule S3 (Security Requirements), then any required change to the ISMS shall be at no cost to the Buyer.

9. VULNERABILITIES AND FIXING THEM

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for the Supplier COTS Software and/or Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within

the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all Supplier COTS Software and/or Third Party COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such Supplier COTS Software and/or Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the IT Environment (to the extent that the IT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.5.12;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the IT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the IT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

9.8

ANNEX 1 – BASELINE SECURITY REQUIREMENTS

1. HANDLING CLASSIFIED INFORMATION

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. END USER DEVICES

2.1 When Buyer Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Buyer Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Buyer Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with the Change Control Procedure.

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Buyer Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Buyer Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Buyer Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Buyer Data held by the Supplier when requested to do so by the Buyer.

4. ENSURING SECURE COMMUNICATIONS

4.1 The Buyer requires that any Buyer Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using

a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY BY DESIGN

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Buyer Data.

5.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the IT Environment (to the extent that the IT Environment is within the control of the Supplier).

6. SECURITY OF SUPPLIER PERSONNEL

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Buyer Data.

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Buyer Data except where agreed with the Buyer in writing.

6.4 All Supplier Personnel that have the ability to access Buyer Data or systems holding Buyer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Supplier Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. RESTRICTING AND MONITORING ACCESS

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the IT Environment (to the extent that the IT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the IT Environment that they require. The Supplier shall retain an audit record of accesses.

8. AUDIT

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the IT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 months.

S6 BUSINESS CONTINUITY AND DISASTER RECOVERY

.1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"BCDR Plan"	has the meaning given to it in Paragraph 2.1 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.2.2 of this Schedule;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.2.3 of this Schedule;
"Related Supplier"	any person who provides services to the Buyer which are related to the Services from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

2.1 At least ninety (90) Working Days after the Commencement Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

2.1.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and

2.1.2 the recovery of the Services in the event of a Disaster

2.2 The BCDR Plan shall be divided into three sections:

2.2.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

2.2.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

2.2.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

2.3 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Services and any goods and/or services provided to the Buyer by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of the Services and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of the Services with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Sub-Contractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Services are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Services and the business operations supported by the provision of Services.

3.4 The Supplier shall not be entitled to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Services remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of the Services; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of the Services in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Services;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services; and

4.2.3 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Sub-Contractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

5.2.11 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.12 testing and management arrangements.

6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

6.1.1 on a regular basis and as a minimum once every six (6) months;

6.1.2 within three (3) calendar months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 8; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year;

7.1.2 in the event of any major reconfiguration of the Services; and

7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Sub-Contractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

S7 CONTINUOUS IMPROVEMENT

1. SUPPLIER'S OBLIGATIONS

1.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Services with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Services and their supply to the Buyer.

1.2 The Supplier must adopt a policy of continuous improvement in relation to the Services, which must include regular reviews with the Buyer of the Services and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Services. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

1.3 In addition to Paragraph 1.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Services and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's approval. The Continuous Improvement Plan must include, as a minimum, proposals:

1.3.1 identifying the emergence of relevant new and evolving technologies;

1.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

1.3.3 new or potential improvements to the provision of the Services including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Services; and

1.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Services, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

1.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for approval within six (6) Months following the Commencement Date, whichever is earlier.

1.5 The Buyer shall notify the Supplier of its approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

1.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

1.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Change in accordance with the Change Control Procedure and the Supplier must implement such Change at no additional cost to the Buyer.

1.8 Once the first Continuous Improvement Plan has been approved in accordance with Paragraph 1.5:

1.8.1 the Supplier shall use all reasonable endeavours to implement any agreed services in accordance with the Continuous Improvement Plan; and

1.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

1.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 1.3.

1.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

1.11 Should the Supplier's costs in providing the Services to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Services.

1.12 At any time during the Contract Period of this Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.