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 3rd August 2022 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 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. 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).

Section A
General information

Contract Details	
Contract Reference:	**CCTS22A41**
Contract Title:	**Provision of TrIS2022 End User Compute**
Contract Description:	**Provision of TrIS2022 End User Compute**
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	**£4,530,297.00 (ex VAT)**
Estimated Year 1 Charges:	**£1,008,293.00 (ex VAT)**
Commencement Date: this should be the date of the last signature on Section E of this Order Form	**8th August 2022**

Buyer details
Buyer organisation name HM Treasury
Billing address Accounts Payable, HM Treasury, Rosebery Court, St Andrew's Business Park, Norwich, NR7 0HS.
Buyer representative name REDACTED TEXT under FOIA Section 40, Personal Information
Buyer representative contact details REDACTED TEXT under FOIA Section 40, Personal Information
Buyer Project Reference To be confirmed

Supplier details
Supplier name Centerprise International Limited
Supplier address Centerprise International Limited Hampshire International Business Park Lime Tree Way Chineham Basingstoke

Hampshire
RG24 8GQ

Supplier representative name
REDACTED TEXT under FOIA Section 40, Personal Information

Supplier representative contact details
REDACTED TEXT under FOIA Section 40, Personal Information

Order reference number or the Supplier's Catalogue Service Offer Reference Number
To Be Confirmed

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

Section B
Part A – Framework Lot

Framework Lot under which this Order is being placed	
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

Initial Term	**Extension Period (Optional)** Months
Three (3) years (8 August 2022 – 7 August 2025)	There is an option to extend for up to two (2) further years in One (1) year Increments

Minimum Notice Period for exercise of Termination Without Cause
see Clause 35.1.9 of the Call-Off Terms

Sites for the provision of the Services

The Supplier shall provide the Services from the following Sites**:**

Buyer Premises:
Please refer to TrIS2022 End User Compute Specification, Annex 1 (Customer Premises) for full list of Her Majesty's Treasury locations.

Supplier Premises:
To Be Confirmed

Third Party Premises:
Not Applicable

Buyer Assets

The Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Services details.
The Buyer Assets are detailed in the attachment "TrIS2022 Bid Support – Reference Data"

Additional Standards

Not Applicable

Buyer Security Policy

Please see Attachment 1 – Statement of Requirements, section 16 - Security & Confidentiality Requirements.

Buyer ICT Policy

Please see Annex 2 - HM Treasury ICT Policy Overview

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 (£5,000,000)

Professional Indemnity Insurance (£5,000,000)

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

Please refer to Services Specification – Part A EUC Services (Customer Obligations) and Services Specification Part B Working with the Customer's Other Suppliers

Goods
Provision of TrIS2022 End User Compute

Pricing Details
REDACTED TEXT under FOIA Section 43 Commercial Interests.

Governance – Option Part A or Part B

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

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

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

The Part selected above shall apply to 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 £0 and
- for the purpose of Paragraph 8.2.2, the figure shall be £150,000.

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	X
S3: Security Requirements (either Part A or Part B)	Part A ☐ or Part B X
S4: Staff Transfer	X
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.

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.

Supplier's security management plan to be added post contract award.

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.

To be confirmed

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.

Supplier personnel shall be subject to pre-employment checks that include, as a minimum, identify unspent criminal convictions and the right to work.

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

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.*

The entire Supplier's Response is to be commercially sensitive information.

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 TEXT under FOIA Section 40, Personal Information
Job role/title	REDACTED TEXT under FOIA Section 40, Personal Information
Signature	REDACTED TEXT under FOIA Section 40, Personal Information
Date	**2nd August 2022**

For and on behalf of the Buyer

Name	REDACTED TEXT under FOIA Section 40, Personal Information
Job role/title	REDACTED TEXT under FOIA Section 40, Personal Information
Signature	REDACTED TEXT under FOIA Section 40, Personal Information
Date	**3rd August 2022**

Attachment 1 – Services Specification

1. PURPOSE

.2 HM Treasury (HMT) is seeking a specialist supplier to deliver an End User Compute (EUC) managed service. The expectation is that EUC will provide an integrated and ubiquitous digital workplace experience that promotes the digital dexterity of end users, supports employee engagement and agility through a more consumerised/digital work environment. EUC provides the core of the TrIS service from a registered user perspective, focusing on delivering the majority of service functions for users to access TrIS services. This service will be underpinned by industry best practices.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

.3 The Customer is the United Kingdom's economics and finance ministry. It is responsible for formulating and implementing the Government's financial and economic policy.

.4 HM Treasury is supported by a shared service function to fulfil all of its Information Communications Technology (ICT requirements). The ICT services are provided by the Information and Workplace Solutions (IWS) Team in conjunction with the Customer's outsourced providers.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

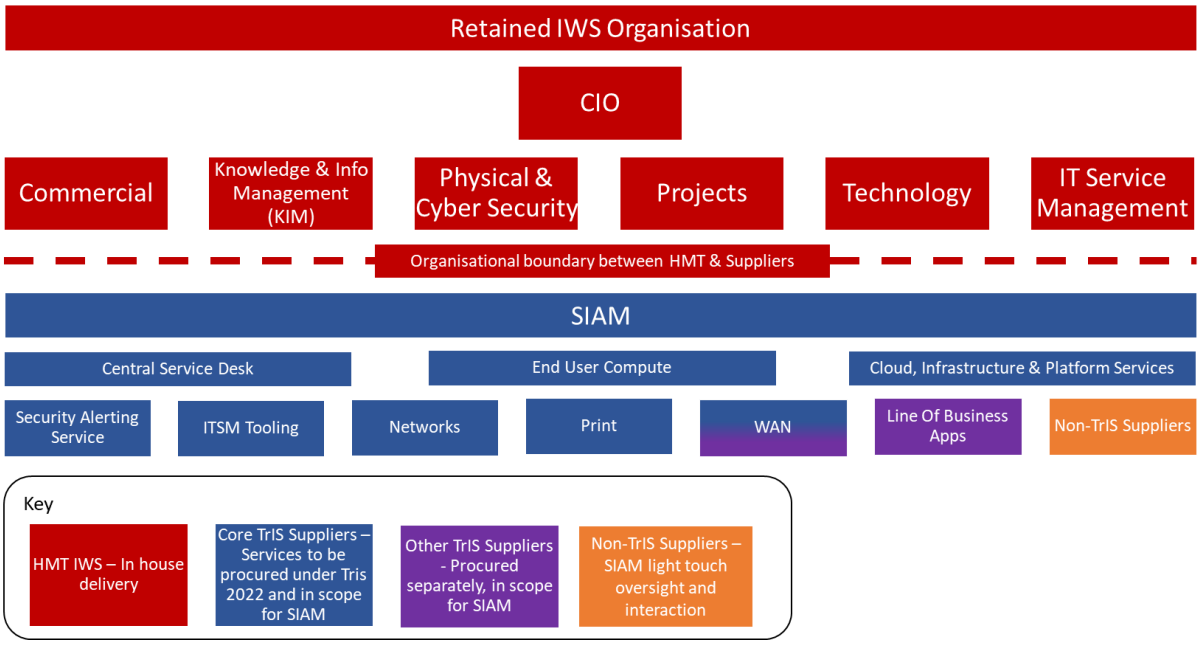
.5 ICT services for the Treasury are provided under the service name Treasury ICT Services (TrIS). TrIS plays a central role in supporting the Treasury in delivering its objectives. TrIS also supports several Arm's Length Bodies (ALBs), including Government Internal Audit Agency (GIAA), UK Government Investment (UKGI), National Infrastructure Commission (NIC) and the Office of Tax Simplification (OTS) in delivering their objectives.

.6 The mass shift to remote working as a result of Covid-19 has highlighted the importance of reliable, flexible enterprise IT as a fundamental bedrock for organisations across all roles and levels. HM Treasury requires a fit for purpose enterprise level 'Official' IT system for the Treasury and it's ALBs in place before current contracts expire for in-scope services. Our approach is to use a manageable number of specialist suppliers to deliver what they are good at, resulting in more effective and efficient services for the department.

.7 Further disaggregating our services will support the ongoing transformation of our workplace, contributing to more efficient delivery by packaging services into smaller groupings, which can be delivered by specialist suppliers through 'best of breed' contracts. The programme of work – known as TrIS2022 - will redesign and

recontract IT services for HMT's main enterprise 'Official' system as per Service Model in Figure 1.

.8 **Figure 1. Service Model**



.9

4. DEFINITIONS

Expression or Acronym	Definition
Acceptable Use Policy	HMT's Technology Policy (and IT Acceptable Use Policy)
Actual Service Commencement Date	in relation to an operational Service, the later of: a) the date identified in the Operational Services Implementation Plan upon which the Operational Service is to commence; and b) where the Implementation Plan states that the Supplier must have Achieved the relevant ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier achieves the relevant ATP Milestone
Applications	the Line of Business Applications and the Core Applications together
ATP Milestone	the Milestone linked to Authority to Proceed for the relevant Operational Services. That is the Actual Operational Services Commencement Date.
Authority	The public body buying works goods or services (formally referred to as a contracting authority in the Public Contracts Regulations 2015).

Automatic Call Distribution or ACD	An automated call distribution system, commonly known as automatic call distributor, a telephony device that answers and distributes incoming calls to a specific group of terminals or agents within an organisation.
AV	Audio/visual
Availability	the ability of a Configuration Item or Service to perform its agreed function when required as determined by reliability, maintainability, serviceability, performance and security. Availability is usually calculated as a percentage based on Service Hours and Downtime.
Call	a contact made to the Central Service Desk via any method, including (but not limited to) phone calls, emails and other self-service mechanisms, which ultimately shall be categorised as either an Incident, Service Request, Problem or Change.
Central Service Desk	the service desk provided by the Central Service Desk Supplier
Commercial Change	any change to this Agreement other than an Operational Change including: a. any change to the Customer's Requirements including any change to the Applications, the End User Devices or the operating system software for the End User Devices; and b. any additional services ordered by the Customer from the Supplier, including any new consultancy services ordered or any new Project ordered by the Authority
Change Advisory Board or CAB	a team comprising of Supplier and Customer personnel who approve requested changes and assist in the assessment and prioritisation of changes
Change Request	a written request for a Commercial Change substantially in the form of Annex 1 of Schedule 5 (*Change Control Procedure*)
CIO	Chief Information Officer
CIPS	Cloud, Infrastructure and Platform Services
Commercial Change	any change to this Agreement other than an Operational Change including: a. any change to the Customer Requirements including any change to the Applications, the End User Devices or the operating system software for the End User Devices (currently. Microsoft Windows); and

	b. any additional services ordered by the Customer from the Supplier, including any new consultancy services ordered or any new Project ordered by the Customer
Complaints	a Call notifying the Central Service Desk of a complaint regarding the Services
Configuration Item or CI	Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management
Configuration Management Database or CMDB	a configuration management database (CMDB) used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items, and relationships with other configuration items.
Continual Improvement	as defined in ITIL4
Core Hours	08:00 to 18:00 Monday to Friday (excluding UK bank holidays)
Core TrIS Services	The services that form the core TrIS service delivery including; Central Service Desk, Print, Network Management, End User Compute, Security Alerting Service, ITSM Toolset and the CIPS service.
Core TrIS Supplier	a supplier delivering any of the Core TrIS Services and falling under the management and reporting remit of the SIAM supplier
Critical Periods	the periods of time before and following the Customer's presentation to Parliament of major fiscal events, these being the Budget and the Autumn Statement, but in exceptional circumstances other events. The dates of major fiscal events vary from year to year and will be advised by the Customer. The Critical Periods will not exceed eight weeks in any calendar year unless where otherwise agreed via Schedule 5 (*Change Control Procedure*)
Customer	shall have the same meaning as Authority, and shall be used interchangeably
Customer Care Initiative	Refers to the work of looking after Users and ensuring their satisfaction with one's service.
Customer Cause	any breach by the Customer of any of the Customer Responsibilities, except to the extent that such breach is:

	a) the result of any act or omission by the Customer to which the Supplier has given its prior consent; or b) caused by the Supplier, any Sub-contractor or any Supplier Personnel
Customer Data	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which: a) are supplied to the Supplier by or on behalf of the Customer; and/or b) the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or c) has been created and saved by Users, using any of the Applications any Personal Data for which the Customer is the Data Controller
Customer Premises	premises owned, controlled or occupied by the Customer which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them).
Customer Provided Software	software which is owned by or licensed to the Customer (other than under this Agreement) and which is or will be used by the Supplier for the purposes of providing the Services, as listed in TrIS2022 Services Specification - Annex 2 (Records and Initial Configuration)
Cyber Security Incident	An event that may result in the integrity and/or availability of an organization's IT systems and the information or data stored/processed on them being compromised, or which may demonstrate that measures put in place to protect them have failed.
Deliverable	an item or feature (such as means any Software, Hardware, Documentation, reports, drawings, calculations, recommendations and conclusions) delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Agreement.
Disaster	a hazard that results in the loss of any main platform used to provide the Services for an extended or unknown period that (in the reasonable opinion of the Supplier) justifies the invocation of the Supplier's Disaster Recovery Plan for the affected platform
Dispute Resolution Procedure	the dispute resolution procedure set out in Schedule 4 *(Dispute Resolution Procedure)*
DPA	Data Protection Act or Data Protection Legislation

End User Device Peripherals	All user device peripherals such as microphones, headphones, card readers and peripheral devices, and all associated equipment used by the Users whether virtual or physical
End User Devices	all User access devices such as desktop PCs, tablets, laptops, Remote Access Devices, as referred to in the CMDB used by Users whether virtual or physical
Enquiry	Refers to a request for information, or the process of seeking information.
Escalation Management	Refers to the process of prioritizing customer service concerns, ranking issues based on severity and ensuring that they're addressed by the right representative.
First Contact Resolution	Refers to the capability of the Service Desk to resolve Users Calls first time, without the need for further follow-up or a call back.
First Level Support	Refers to the Service Desk, who are responsible for Incident registration, routing service requests to support groups when Incidents are not closed, initial support and classification, ownership, monitoring, tracking and communication, resolution and recovery of Incidents not assigned to second-line support, and closure of Incidents.
First Time Fix Rate	Refers to the percentage of time a technician is able to fix the issue the first time, without need for additional expertise, information, or parts.
Freedom of Information Act or FOIA	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Central Government Body in relation to such Act
Goods	means goods or equipment to be sold to the Customer by the Supplier as part of the Services
Government Buying Standards and requirements under the UK Greening government: ICT and digital services strategy (2020-2025 or successor);	A set of sustainable mandatory minimum standards and best practice specifications for a range of commonly-purchased products by government, such as IT equipment, white goods, paper etc
Greening Government Commitments	As described at https://www.gov.uk/government/collections/greening-government-commitments
HMG Security Policy Framework	As described at https://www.gov.uk/government/publications/information-security-policy-framework

HMT	means Her Majesty's Treasury
ICT	means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony
Incident	a) an unplanned interruption to the Customer's IT or a reduction in the quality of its IT; or b) failure of a configuration item that has not yet impacted on the Customer's IT, and Incidents will be construed accordingly
Information	all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form)
Information and Security Management	The application of controls within an organisation to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.
Interactive Voice Response or IVR	Refers to an automated phone system that allows incoming callers to access information via a voice response system.
ISO	International Organisation for Standardisation
IT Health Check or CHECK IT Health Check	A 'penetration test' carried out by an independent body to assess any vulnerabilities to the Customer's ICT environment
IT Infrastructure	The system of hardware, software, facilities and service components that support the delivery of business systems and IT-enabled processes.
ITIL	the IT Infrastructure Library (ITIL) IT service management best practice framework – where key terms and acronyms of ITIL are used in this contract set they shall have the meaning as defined in ITIL, unless otherwise defined in this table.
ITSM	Information technology service management
Known Errors	means a condition identified by successful diagnosis as the root cause of a problem, and the subsequent development of a workaround

Main London Premise	HMT's premises at 1 Horse Guards Road, London, SW1A 2HQ
Major Cyber Incidents	An event that may result in the integrity and/or availability of an organization's IT systems and the information or data stored/processed on them being compromised to a very significant extent, and/or which may demonstrate that measures put in place to protect them have failed in a very big way.
Major Incidents	As defined by ITIL4
Milestone Date	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved
Multi-Functional Device (MFD)	A network connected office machine that combines multiple functions in a single device including print, scan copy and scan to email capabilities and serves large workgroups
NCSC	National Cyber Security Centre
NCSC Information Security Guidance	Information Security policies and guidance, issued by the National Cyber Security Centre.
Non-TrIS Supplier	any relevant suppliers with whom the Customer enters into agreements other than the Core TrIS Suppliers and the Other TrIS Suppliers (e.g. the facilities management supplier).
Operational Change	means a change in how the Services are to be provided by the Supplier or any change in the Supplier Solution, that does not result from a change in the Customer's Requirements
Other Suppliers	Suppliers with whom the Customer enters into agreements other than the Supplier i.e.: a) the Core TrIS Suppliers b) the Other TrIS Suppliers; and c) the Non-Tris Suppliers.
Other Supplier's Services	the services provided by the Other Suppliers.
Other TrIS Supplier	any supplier providing a service related to the TrIS Services, except those defined as a Core TrIS Service (e.g. a COTS software supplier)
PABX	Private Automatic Branch Exchange
Parliamentary Questions	A formal parliamentary question asked to the department by an MP. A formal response is required within two days of receiving the question
Person Day Rates	the rates of the Supplier Personnel or Sub-contractors as set out in Attachment 2 *(Charges and Invoicing)*

Planned Operational Service Commencement Date	the date upon which the Operational Services are to commence, as set out in Schedule S1 *(Implementation Plan).*
POE	Power Over Ethernet
Problem	the underlying cause of one or more Incidents
Projects	means any project to implement a material Commercial Change that affects the Services, including material software development and project management services
Record	Refers to a record containing the details of an Incident/ Problem/ Change or Request, documenting its lifecycle.
Recurring Incident	Refers to an incident that is repetitive in nature, having a similar subject or root cause as another incident(s).
Registered Users	a person with authorised access to the Customer's network (the number and identity of such persons to be managed pursuant to a procedure agreed by the Parties), registered as a recipient of the Services. Service Charges (as defined in Attachment 2 *(Charges and Invoicing)*) shall not apply to any Registered User employed or engaged by either the Supplier, or by any Other Supplier, for the purposes of delivering any part of the TrIS Services.
Release	a software or hardware release produced by a third party, a release produced by the Supplier at its own initiative or a release developed by the Supplier for the Customer as part of a Project.
Relevant Infrastructure	the infrastructure to be provided by the relevant Supplier
Relevant Services	the services to be provided by the relevant Supplier
Remote Access Devices	any approved or configured mobile phone, smartphone, or other device that can connect to and operate on a mobile network in order to connect to the TrIS Services
Risk Register	the register of risks and contingencies that will be agreed between the Parties under the Risk Management Service
Root Cause Analysis or RCA	means a well-documented method of problem solving that tries to identify the fundamental (root) cause of an incident or a problem.
SAS	Security Alerting Service
SC Security Check Level	National Security Vetting: Security Check (SC) clearance level. As described in https://www.gov.uk/government/publications/united-kingdom-

	security-vetting-clearance-levels/national-security-vetting-clearance-levels
Scheduled Maintenance	any hardware maintenance and software support set out in the scheduled maintenance plan to be prepared by the Supplier under the Scheduled Maintenance Service
Scheduled Outages	any scheduled outages agreed with the Customer to carry out Scheduled Maintenance
Security Incident	An event that may result in the integrity and/or availability of an organization's IT systems and the information or data stored/processed on them being compromised, or which may demonstrate that measures put in place to protect them have failed.
Security Management Plan	the Supplier's security plan as developed and revised in accordance with the obligations of the Security Management Coordination & Oversight Service
Security Requirements	as set out in HMT TrIS Security Management Plan, the Services Specification, the Order Form, the HMT ICT Policy and Schedule S3 – Security Requirements
Self Service Portal	Refers to a place where Users have the ability to find answers to their inquiries, fix their own incidents, raise their own support tickets, and even help their colleagues by promoting a culture of knowledge sharing and collaboration.
Service Catalogue	the service catalogue provided by the Supplier setting out the ICT Goods and Services available to the Customer or to Registered Users as an orderable item.
Service Delivery Lifecycle	Refers to the end-to-end delivery of the IT Service.
Service Delivery Managers	managers assigned by the Supplier to carry out management of the Services
Service Desk	See Central Service Desk definition
Service Events	Refers to an instance or occasion of assistance received by a User.
Service Hours	the service hours set out in each Service Line during which the services described in the Service Line shall be available to the Customer.

Service Improvement Plan	a plan created by the Supplier setting out how it proposes day to day enhancement of the service in accordance with the Quality Management and Service Improvement Service
Service Knowledge Management System	Refers to an IT system that stores and retrieves knowledge to improvement understanding, collaboration and process alignment.
Service Level	the service levels set out in Attachment 4 – Service Levels and Service Credits
Service Request	a request from a User to receive a Service that is to be provided by the Supplier on request;
Services	any and all of the services to be provided by the Supplier under this Agreement, including those set out in Attachment 1 of the Order Form - *Services Specification*
SIAM	Service Integration & Management
SKU	a distinct item, such as a good, product or service, as it is offered for sale or supply and which embodies all attributes associated with the item and that distinguish it from all other items, and thus also act as a unique identifier for inventory management
SOC	Security Operations Centre
Standard Operating Environment	standard implementation of an approved operating system and its associated software
STAR (Sustainable Technology Annual Report)	As described at https://www.gov.uk/government/publications/greening-government-ict-sustainable-technology-annual-report-2018-to-2019
Supplier Default	any default by the Supplier of its obligations under this Agreement
Supported Environments	The Supported Environments are: a) the live (production) environment; b) a pre-production (development) environment for all systems; c) those environments needed to meet other requirements in the Services Specification and Schedule S6 (*Business Continuity & Disaster Recovery*); and/or

	any other testing and service environments as may be necessary to ensure the on-going provision of fully functional, tested, proven, accepted, and reliable services required for business as usual and for the introduction of new ICT services (including patching, application of service packs and the release of updated and/or upgraded applications, software, operating system components and firmware);
Supported Systems	means all the hardware, software and systems supported or maintained by the Suppliers
Sustainable ICT and digital services strategy: targets for 2020-2025 (or successor);	As described at https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025
Time and Materials	means where the Charges are based on the actual cost of Man Hours used to provide Services and the actual cost of any materials and equipment used in providing the Services
TBS	Treasury Business Solutions, previously known as IWS (Information & Workplace Solutions)
TrIS Infrastructure	the ICT systems used by the TrIS Suppliers in implementing and performing the TrIS Services including all software, equipment, configuration and management utilities, calibration and testing tools and related cabling, whether provided by the Tris Suppliers, a Non-TrIS Supplier, or the Customer, and including the TrIS Infrastructure.
TrIS Services	the services provided by the TrIS Suppliers and the Other Suppliers.
TrIS2022	Treasury Information Systems 2022 Project
UK GDPR	General Data Protection Regulation (UK GDPR). The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
UK Greening government: ICT and digital services strategy (2020-2025 or successor);	As described at https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025
Unclassified Loan Devices	all User access devices, (including desktops, laptops, tablets, mobile phones, smartphones) that are managed via

	a loan service and are not used to connect to the TrIS services
URL	Uniform Resource Locator
User Feedback Survey	a survey created and implemented in accordance with Attachment 1 - TrIS2022 Services Specification SIAM Specification – User Feedback and Surveys Service
Users	a Registered User or another user as nominated by the Customer
Video-Conferencing Equipment (VC)	unless otherwise stated includes video-conferencing equipment and TelePresence equipment and associated peripherals (such as remote control units) listed in the CMDB.
VIPs	Very Important Person - an important User, as nominated by the Customer
VOIP	Voice over Internet Protocol
Working Day	means any day other than a Saturday, Sunday or UK bank or public holiday
Workplace Adjustment or Reasonable Adjustment	as defined under the Equality Act 2010 and which is identified by the completion of an Access to Work, Occupational Health or DSE workstation assessment, which has been approved by the Customer.

5. SCOPE OF REQUIREMENT

.10 As described against each of the services in Attachment 3b - TrIS2022 End User Compute Specification Part A, sections 1 – 27.

6. THE REQUIREMENT

.11 As described in Attachments 3b, c, d & e - TrIS2022 End User Compute Specification.

7. KEY MILESTONES AND DELIVERABLES

.12 The following Contract milestones/deliverables shall apply:

.12.1 Milestone/Deliverable	.12.2 Description	.12.3 Timeframe or Delivery Date

.12.4	1	.12.5	Provide name and contact details of Supplier Data Protection Officer	.12.6 Within 1 working day of Contract Award
.12.7	2	.12.8	Meet with SIAM supplier to confirm proposed solution	.12.9 Within 5 working days of Contract Award
.12.10	3	.12.11	Deliver draft 30-60-90 day implementation plan for Customer approval	.12.12 Within 20 working days of Contract Award
.12.13	4	.12.14	All integration of tools and processes completed	.12.15 29th August 2022
.12.16	5	.12.17	Services ready to transfer to live service	.12.18 28th Sept 2022
.12.19	6	.12.20	Provide an analysis paper based on baseline data, highlighting potential recommendations to service improvements which may result in process / cost efficiencies to be agreed by HMT	.12.21 90 days after contract award

8. MANAGEMENT INFORMATION/REPORTING

.13 Please refer to Attachment 3e - TrIS2022 End User Compute, Annex 3 (Reports).

9. VOLUMES

.14 Please refer to the Bid Support Reference Data (Attachment 6)

10. CONTINUOUS IMPROVEMENT

.15 Please refer to Attachment 3c - TrIS2022 End User Compute,

.16 Part B, 32 Continual Improvement and Innovation Service

11. SUSTAINABILITY

.17 Please refer to Attachment 3c - TrIS2022 End User Compute, Part B Section 47 (Sustainability Service).

12. QUALITY

.18 Please refer to Attachment 3c - TrIS2022 End User Compute, Part B Section 49 (Quality Management Service).

.19 The supplier shall ensure their processes and procedures are ITIL aligned and conform with ISO/IEC 20000 and ISO/IEC 27001, and that they are Cyber Essentials certified.

13. PRICE

.20 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

14. STAFF AND CUSTOMER SERVICE

.21 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

.22 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

.23 The Supplier shall ensure that staff understand the Customer's vision and objectives and will provide excellent customer service to the Customer throughout the duration of the Contract.

15. SERVICE LEVELS AND PERFORMANCE

.24 The Customer will measure the quality of the Supplier's delivery by: please refer to Attachment 3d - TrIS2022 End User Compute, Part C – Service Levels

16. SECURITY AND CONFIDENTIALITY REQUIREMENTS

.25 The Supplier acknowledges that the Customer places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Supplier Provided Infrastructure. The Supplier also acknowledges the confidentiality of Customer Data.

.26 The Supplier shall be responsible for the security of the IT Environment and shall at all times ensure a level of security which:

(i) is in accordance with Good Industry Practice and Law;

(ii) ensures the Customer can comply with the HMG Security Policy Framework;

(iii) is compliant with any mandated Code of Connection requirements;

(iv) meets any specific security threats to the IT Environment, ;

(v) complies with Information Assurance Standards;

(vi) complies with the detail of the Customer's Security Policy and;

(vii) ensures that usability is at the forefront of design and implementation.

.27 Without limiting paragraph 1.2, the Supplier shall at all times ensure that the level of security employed in the provision of the Goods and/or Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Customer):

(i) loss of integrity of Customer Data;

(ii) loss of confidentiality of Customer Data;

(iii) unauthorised access to, use of, or interference with Customer Data by any person or organisation;

(iv) unauthorised access to network elements, buildings, the Premises, and tools used by the Supplier in the provision of the Goods and/or Services;

(v) use of the Supplier Provided Infrastructure or Goods and/or Services by any third party in order to gain unauthorised access to any computer resource or Customer Data; and

(vi) loss of availability of Customer Data due to any failure or compromise of the Goods and/or Services.

.28 The Supplier shall ensure that all Customer Data be held on-shore within the UK at all times. The Supplier shall provide evidence to the Customer on request as soon

as possible and in any event no later than within 72 hours of any such request, and shall provide a written statement to this effect, at least annually.

.29 The Supplier shall, without prejudice to its other obligations in the Agreement, provide a continuous and comprehensive Security Management service, in the event of a Business Continuity or Disaster Recovery situation.

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

.31 Supplier personnel shall be subject to pre-employment checks that include, as a minimum, identify unspent criminal convictions and the right to work.

.32 The Supplier shall conform to the following security clearance conditions for Supplier Personnel who, when working for the Customer, will:

(i) be expected to have systems administration rights to the IT Environment, must have a minimum security clearance of SC (Security Check) which also requires BPSS (Baseline Personnel Security Standard) as part of this clearance;

(ii) be expected to work in the Delivery Locations unsupervised and/or who will require normal user access to the IT Environment must have a minimum security clearance of BPSS CTC (Counter Terrorist Check) which also requires BPSS (Baseline Personnel Security Standard) as part of this clearance; and

(iii) not normally have access to the Delivery Locations but who, are likely to have access to Customer Data, must have a minimum security clearance BPSS CTC (Counter Terrorist Check) which also requires BPSS (Baseline Personnel Security Standard) as part of this clearance. Higher levels of security clearance will be required for access to information/data of a higher classification than OFFICIAL.

.33 During employment in the Services the Supplier shall ensure that all terms and conditions of employment contracts for Supplier Personnel state their and the Supplier's responsibilities for Security.

.34 All Supplier personnel that can access Customer Data or systems holding Customer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Customer in writing, this training must be undertaken annually.

.35 Where the Supplier or Subcontractors grant 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 staff no longer

require elevated privileges, or leave the organisation, their access rights shall be revoked within 1 Working Day.

17. PAYMENT AND INVOICING

.36 **Please refer to Schedule 2 of the Call-off terms – Charges & Invoicing.**

.37 **Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.**

.38 **Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.**

.39 **Invoices should be submitted to: Invoicequeries@hmtreasury.gov.uk or Accounts Payable, HM Treasury, Rosebery Court, St Andrew's Business Park, Norwich, NR7 0HS.**

.40 **No invoice will be authorised without an associated purchase order number.**

18. CONTRACT MANAGEMENT

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

19. LOCATION

.42 **The location of supplies and services will be pursuant with and in accordance with Attachment 6a Part A. Services will be delivered from Suppliers own premises. However, the Authority reserves the right in its sole discretion to review and alter the Location dependent on requirements through the Contract Change Procedure. Please refer to TrIS2022 End User Compute Specification, Annex 1 (Customer Premises) for full list of Her Majesty's Treasury locations.**

.43

.44

Services Specification Introduction
End User Compute (EUC)

1.1 Customer's Contract Objectives

1.1.1 The Supplier shall provide the Goods and Services to the Customer to satisfy the following objectives (Customer's Contract Objectives):

Transition – effect a smooth transition from the current services with no avoidable adverse impact on the Customer's business;

Quality - deliver an uninterrupted service to Customer staff that meets business requirements and minimises business disruption, as documented in this Agreement;

Cooperation and coordination – ensure that the Services are provided by the Supplier in close co-operation with and are co-ordinated with the Other Suppliers in both the letter and the spirit of the Agreement;

Continual improvement – ensure continual improvement in the quality of the Services both strategically and through day-to-day enhancement, in accordance with the *Continual Improvement & Innovation Service*

Cost – ensure that the Charges are competitive and aligned with market price;

Cost certainty – the Customer's needs have been defined so that the Charges are defined and predictable and that the number of Change Requests is reduced to the absolute minimum;

Better management information – provide accurate and detailed management information about the Services to assist the Customer to perform its functions (as set out in this Services Specification);

Flexibility – provide flexible and proactive ICT services to deal with the potential changes in the Customer's locations, data and Users including ensuring that the Supplier's Solutions are designed to allow the separation of the three different parts of the Services so that individual parts can be benchmarked, terminated or extended;

Scalable - provide a scalable service that other Public Sector organisations could join in the future. The Customer shall act as prime customer in respect of all services provided to any joining Government departments;

Reduce risk – provide resilient and robust ICT services; and

Security – provide the Services and Goods in a safe and secure manner and in particular comply with the security obligations set out in this Agreement.

1.2 VIPs

1.2.1 The Customer will nominate specified Registered Users, who have significant influence over the perception of the Services within the Customer as VIP

1.2.2 The Supplier shall:

(a) observe the record of nominated VIPs so that they can be recognised when they raise Incidents or Service Requests;

(b) ensure that it and Other Suppliers provides a particularly attentive service to VIPs, including ensuring that any Incidents or Service Requests raised by a VIP are prioritised alongside other Incidents or Service Requests of the same Priority Level;

1.3 Service Hours

1.3.1 The Supplier shall provide the Services during the Service Hours specified in respect of each Service Line.

1.4 General obligations

1.4.1 Where this Services Specification states that the Supplier shall agree processes or documentation with the Customer or with Other Suppliers, the Supplier shall act reasonably in agreeing the relevant processes or documentation.

1.4.2 Where this Services Specification states that the Supplier shall keep records, reports or other documentation, the Supplier shall ensure that the records, reports or other documentation are complete and accurate and are up-to-date (i.e. no more than 5 Working Days out of date unless otherwise specified in this Schedule or agreed with the Customer).

1.4.3 Where this Services Specification states that the Supplier must obtain the Customer's approval or agreement, the Supplier shall obtain the Customer's approval or agreement in writing.

1.5 Changes requiring consent

1.5.1 The Supplier may not change its solution without the consent of the Customer. The Customer shall not unreasonably withhold or delay its consent unless the change relates to material aspects of the Supplier's Solution. The Customer shall be regarded as reasonably withholding its consent if the Customer reasonably believes that the proposed change would:

1

(a) materially increase the Customer's risk including reputational risk or the risk that the Supplier or any of the Other Suppliers shall not meet the timescales set out in the Implementation Plan or in any of the Project Plans;

(b) conflict with security accreditation requirements or increase security risks;

(c) result in the Customer incurring any additional or increased costs or expenses;

(d) result in a change in the Goods or Services;

(e) adversely affect the relevant Supplier's ability to provide the Services at all or to provide them to the Service Levels;

(f) adversely affect the ability of Other Suppliers to provide their services to the Customer;

(g) reduce the effectiveness of the governance provisions of this Agreement;

(h) adversely affect the Customer's ability to ensure a smooth transition on Termination;

(i) or adversely affect the ability of the Supplier to comply with any of its other obligations under this Agreement.

1.5.2 Without prejudice to this Paragraph or any other provisions of this Agreement, any change in the way in which the Supplier provides the Goods and/or Services will require the Customer's prior written approval if it would:

(a) materially increase the Customer's risk including reputational risk or the risk that the Supplier or any of the Other Suppliers shall not meet the timescales set out in the Implementation Plan or in any of the Project Plans;

(b) conflict with security accreditation requirements or increase security risks;

(c) result in the Customer incurring any additional or increased costs or expenses;

(d) result in a change in the Goods or Services;

(e) adversely affect the relevant Supplier's ability to provide the Services at all or to provide them to the Service Levels;

(f) adversely affect the ability of Other Suppliers to provide their services to the Customer;

(g) reduce the effectiveness of the governance provisions of this Agreement;

(h) adversely affect the Customer's ability to ensure a smooth transition on Termination; or

(i) adversely affect the ability of the Supplier to comply with any of its other obligations under this Agreement.

1.6 Provision of assets and premises

1.6.1 Except to the extent stated to the contrary in this Services Specification the Supplier shall provide, maintain and replace all Supplier infrastructure, information and communications technology systems, assets, tools and consumables necessary for the proper and efficient performance of the Relevant Services and the procurement of the Goods.

Supplier Sites

1.6.2 Except where something different is specified in this Services Specification, the Supplier shall provide all premises necessary for the proper and efficient performance of the Services.

1.6.3 Subject to:

(a) any requirement for the on-site delivery of Goods and Services in this Services Specification

(b) any requirement for Key Personnel be present on site if needed – as specified in Attachment 5 (*Key Personnel and Key Sub-Contractors)*

(c) any Customer Premises being made available to the Supplier under in Part B of this Services Specification (Working with the Customer and Other Suppliers); or

(d) any right in the agreement between the Customer and the Supplier to change the site from which the Services will be provided.

1.6.4 The Supplier shall provide the Goods and Services from the Supplier Sites agreed between it and the Customer.

1.7 Dependencies on the Other Suppliers

1.7.1 The service description in this Services Specification includes a column entitled "Other Suppliers' obligations". These obligations on Other Suppliers are set out in the contract between the Customer and the relevant Other Supplier.

1.7.2 The Customer will make reasonable efforts to enter into Agreements with the Other Suppliers to ensure they will deliver their obligations as described in the 'Other supplier's obligations' column and Part B of this document.

1.7.3 For the avoidance of doubt, all references to 'Other Suppliers' within this Services Specification mean the Core TrIS Suppliers as described in the Definitions, unless stated otherwise

1.8 Customer Responsibilities

1.8.1 The service descriptions in this Schedule also include a column entitled "Customer Obligations". These are in addition to obligations listed in Part B of this Services Specification (Working with the Customer and Other Suppliers)

Part A Services - End User Computing Services

1. End User Support Service

The End User support function shall provide operational assistance to handle queries from the Customer, the Customer's Users, and Other TrIS Suppliers on technology-related systems, processes, policies, or usage. Services may include skilled product capabilities, including hardware and software support elements, dispatch of service technicians and/or parts, end-user training coordination and other technology-related activities.

The main aim of end user support is to provide Users with assistance in a timely manner by analysing requests and attending to them quickly and accurately. The scope of these services shall deliver a comprehensive set competence and shall be capable of delivering;

i. remote diagnosis and resolution of hardware and/or software related Incidents and Service requests;
ii. field support and deskside visits to support Users at agreed HMT locations or non-Customer premises (ad hoc) as required;
iii. proactive analysis of problem trends to suggest permanent fixes; and
iv. provision of advice and guidance to Users in the practise of End User Computing

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
1.1 **Outline** To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
1.2 **Scope**		

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
provide a pool of security cleared, skilled and trained support engineers to support delivery of the TrIS End User Computing Services including but not limited to; End User Support; End User Device Management; and Application Management		
1.3 **Service Hours** 08:00 to18:00 Monday to Friday (excluding UK bank holidays); and Out of hours cover to respond to escalations (Priority 1 and Priority 2 Incidents) as required provide a flexible resourcing model to offer extended hours of service supporting the Customer's Patterns of Business Activity, providing support during Critical Periods 24 hours a day, 7 days a week, 365/6 days a year;	The Customer shall provide 4 weeks' notice of any upcoming Critical Periods.	
1.4 **Standards** deliver all End User Compute Support Services within the confines of the best practice ITIL IT Service Management (ITSM) framework and ensure that the End User Computing function is compliant with relevant ISO/IEC international standards;		
1.5 **Contact Methods** Operating in a multi-supplier provision and support environment by accepting any contact to the End User Computing Services, interfacing with the Customer's ITSM tool,	The Customer shall provide access to their ITSM tool. The Customer shall ensure that ITSM toolset is available	Each of the Other Supplier shall align its processes with the Incident Management Service.

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
either via API (Application Programming Interface) or manually updating the Customer's ITSM tool, in order to; • receive and track Incidents and Service Requests; • respond to Incidents and Service Requests from the Other Suppliers within agreed operational and service levels; • provide real-time service performance status information; and • manage and present service performance reporting provide and maintain a list of Supplier Staff who require access to the Customer's ITSM toolset and their required permission level	and that Supplier user accounts are created with appropriate permissions.	
1.6 **Services** Working with the Customer and the Other Suppliers, the Supplier shall:		
End User Support		
a) provide an End User Support function capable of interacting with the Central Service Desk, the Customer's Users, the Customer, and the Other Suppliers;	The Customer shall provide an ITSM tool and make it accessible to all Suppliers for the purpose of co-	The Central Service Desk Supplier shall provide a Central Service Desk which shall act as the Single Point of Contact for

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
b) provide 2nd and 3rd line technical support to the Customer's Users for Client Software, System Software and hardware equipment including, but not limited to; i. diagnosis and resolution of hardware and/or software Incidents and Service Requests reported by the User either by a remote fix or via deskside visit at agreed HMT locations or non-Customer premises (ad hoc) as required ii. providing guidance on suitable technical workarounds/temporary fixes that enables Users to operate whilst a permanent resolution is being provisioned; iii. support of all Microsoft Office O365 suite applications and other applications as required; iv. respond to requests for on-site technical support as required, such as ad-hoc requests to support Video-Conferencing Equipment; and; v. supporting and/or preparing site-surveys to support workplace moves and provide feasibility advice such as the location having appropriate network connections to support the proposed number of Users; c) action all Service Requests in accordance with the request fulfilment policies, processes and procedures, including but not limited to;	ordinating the End User Support function.	Users to report Incidents and Requests for Service.

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
i. installation or fulfilment of hardware requests (including End User Devices and Peripherals); ii. administration requests related to Remote Access Devices (and, where appropriate, some Unclassified Loan Devices) mobile service networks such as enabling international roaming or porting a number; iii. creation and/or deletion of User accounts (including all requests submitted via the Customer's starters, leavers and movers process); iv. arranging training for Users with Workplace Adjustments in relation to the provided Hardware or Software made available; and v. responding to all requests for Installs, Moves, Adds and Changes and be responsible for implementation as required		
Problem Management		
d) contribute to the Problem management process by employing Root cause analysis to determine cause of Problems and to further eliminate potential issues by implementing a permanent fix for all identified problem causes;	The Customer will provide ITSM tool for the purposes of Problem Management.	The SIAM Supplier shall design and provide a comprehensive Problem Management Oversight service.
Meeting Room Management		
e) routinely perform daily checks of meeting rooms at 1 Horse Guards Road and, at the request of the Customer, other Customer Premises:	The Customer shall agree with the supplier which meeting rooms are in scope	

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
f) regularly checking Customer used End User Devices and Peripherals in meeting rooms before 9am each day (Monday to Friday, excluding UK Bank Holidays) which should include, but not be limited to: i. opening a Test VC call ii. ensuring there is an HDMI cable, or any other equipment required to make a Video-Conferencing call, is in the room iii. ensuring cables are tidy iv. checking that there is good Wi-Fi signal in the room and raise a call with the facilities helpdesk if there is a problem v. ensuring that VC guides are in the room vi. checking, where relevant, that the screen is displaying room info vii. logging and resolving any incidents arising from these checks;	of the Meeting Room Management Service.	
Continual Service Improvement		
g) design, transition, operate and continually improve the Service in accordance with the Continual Improvement and Innovation Service and in accordance with the Service Levels; h) operate wherever possible to improve the resolution of Incidents and fulfilment of Service Requests, ensuring that these are carried out at the earliest point; and wherever possible, move things that are typically done in later stages, earlier; enabling, instigating, and facilitating a continual shift left mentality;		The SIAM Supplier shall provide and maintain a Continual Improvement and innovation plan.
Supporting the Other Suppliers		

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
i) provide the necessary coordination to support the interworking between the SIAM Supplier and Other Suppliers in delivery of the end-to-end TrIS Services which shall include: i. ensuring interoperability in accordance with the Service Integration and Management Oversight plan ii. management and support of software, on End User Devices, provided by the Other Suppliers iii. enabling the Central Service Desk Supplier to remotely access securely onto End User Devices or perform administrative functions as required (including for performing password resets and remote wipes of End User Devices);	The Customer shall provide an ITSM tool and make it accessible to all Suppliers for the purpose of co-ordinating the End User Support function.	The SIAM Supplier shall provide and maintain a Service Integration and Management Oversight plan. The Central Service Desk Supplier shall perform administrative functions and First Level Support for Incidents and Service Requests relating to End User Device access and account management. Each of the Other Suppliers shall, during the implementation and onboarding process, provide the EUC supplier with full details of any software or software functionality that they require, and shall notify the EUC supplier of any subsequent changes to their software or software functionality. Any such changes will be managed in accordance with the Change Control Procedure.
Development of Self-Service		

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
j) actively seek alternative methods to provide self-service facilities in support of the provision and consumption of End User Computing services and implement plans to follow such alternative methods, subject to approval by the Customer;	The Customer shall not delay approval of all suitable alternative self- service methods.	
Customer Care Initiative		
k) provide an up-to-date service guide, directory, locations list and any other content for User training for the video-conferencing service and promote the video-conferencing service to all Users; l) implement and deliver before the Planned Operational Services Commencement Date, and thereafter maintain, a customer care initiative to support the Users and ensure that: i. the End User Computing Support staff respond to Users in a professional and courteous manner; ii. the End User Computing Support staff follow up Complaints and enquiries; iii. the End User Computing Support staff follow up and update the record the Users are able to see with an accurate and meaningful status and ensure that Incidents/Problem/Service Requests and Changes shall be deemed closed only after the User has acknowledged that no further action is required; iv. all End User Computing Support Staff have access to the Service Knowledge Management System, within the Customer's ITSM solution,	The Customer shall provide an ITSM tool and make it accessible to all Suppliers for the purpose of co-ordinating the End User Support function.	

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
and are familiar with all knowledge base articles pertaining to the Customer's services and this shall also be made available to Users as appropriate; m) update and communicate status updates to the User on Incident and Service Request as defined in the Central Service Desk policies and procedures and in accordance with Part B (Working with the Customers Other Suppliers);		
End User Computing Support Staff		
n) ensure that all End User Computing Support staff involved in the delivery of End User Support are suitably security cleared in accordance with the with the Customer's Security Requirements; o) ensure that the End User Computing Support staff are knowledgeable, capable and competent in the operation of the End User Computing, the Customer's services and the Customer's mode of operation and that; i. all End User Computing Support staff have been trained in the use of applicable processes and procedures including customer care initiative; p) ensure that End User Computing Support staff recognise Users may not, by default, be a member of staff and/or office based and adjust their advice appropriately; q) all End User Computing Support staff are familiar with the Customer's business environment and that of the User community they are supporting; and	The Customer shall be responsible for sponsoring vetting of Supplier staff and for agreeing the differing levels of clearance required for different roles. The Customer shall provide guidance and training on the Customer owned ITSM tool.	

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
r) all End User Computing Support staff interacting with the Customer's ITSM toolset are fully trained and capable in the use of the Customer's ITSM toolset for the relevant functions and processes;		
Service Measurement and Reporting		
s) provide a performance monitoring framework capable of providing different perspectives supporting, but is not limited to: i. the use of a monthly Balance Scorecard showing a mixture of quantitative and qualitative measures; ii. comparative analysis of Service performance against past, present and forecast of future predictions; iii. evaluation of the performance of End User Computing Support Services against stated Service Levels, Customer objectives and other agreed performance measures; and iv. sufficient granularity to identify the effects of poor performance and implement service improvements as required; t) ensure performance information provided shall contain, but is not limited to, details of: i. performance over the agreed service reporting period;	The Customer will make data from the Customer owned ITSM tool available to the supplier to support this.	

1. End User Support Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
ii. year to date (over 13 month rolling period); and iii. show an aggregate of performance month on month over a 13 month period		

2. End User Device Management Service

End User Device Management shall provide end-user device and ancillary services to support the delivery of the TrIS Services' and sponsor cloud-first, automated and integrated support to end-users. It shall cover the distribution, management, and maintenance of (but not limited to); End User Devices (including laptops, desktops, and mobile devices), hardware and peripheral equipment. It shall consist of appropriately skilled staff responsible for dealing with a variety of Service Events and should ensure effective and timely management and communication to the User across the portfolio of TrIS EUC Services to achieve the agreed Service Level Targets defined in Part C.

The primary aim of the End User Device Management function shall be to deliver a minimum set of standards for end-user devices and their use within the Customer's environment and ensure that Users are as productive as possible by ensuring that their IT doesn't get in their way. The scope of these services shall deliver a comprehensive set of competences and shall be capable of delivering;

- Spares lifecycle management, including secure storage, maintenance and warranty management;
- Endpoint protection (Patch Management), including antivirus, anti-malware and anti-spam;
- Build, configuration and management of Customer's Standard Operating Environments to Customer specification, including Unclassified Loan Devices;
- Applying Standard Operating Environments (including o/s and software) to End User Devices;
- Deploying core hardware including desktops, laptops, and peripherals, recognising Workplace adjustment needs as required;
- Coordinating End User Device and Peripheral installations, collections, upgrades and moves as required, including Unclassified Loan Devices and Workplace Adjustments;
- Interaction with 3rd Party vendors as required;

The requirements for the End User Device Management Service are listed below:

2. End User Device Management Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
2.1 Outline	The Customer shall be responsible for the disposal of	

Provide an End User Device Management capability for the management of End User Devices and Peripherals in line with industry best practice and NCSC guidance	End User Devices and Peripherals and agree plans for collection of stock.	
2.2 Service Hours 08:00 to18:00 Monday to Friday (excluding UK bank holidays); and Out of hours cover to respond to escalations (Priority 1 and Priority 2 Incidents) as required		
2.3 Scope All End User Devices		
2.4 Services Working with the Customer and the Other Suppliers, the Supplier shall:		
Procurement and Storage of End User Devices		
a) Provide an End User Device Management capability for the management of End User Devices and Peripherals in line with industry best practice and NCSC guidance including but not limited to; i. procurement of End User Devices and Peripherals including Workplace Adjustments hardware and software as required and Video-Conferencing Equipment, in line with the Procurement Service; ii. secure storage of End User Devices and Peripherals at a Supplier location, ensuring;		

	a. the store is tightly controlled to ensure that access to the storage area and content is only possible for authorised personnel b. all equipment in the store is uniquely asset tagged and recorded in an asset register c. Any losses or theft of equipment are reported to the Customer as soon as the Supplier becomes aware of them d. stock and inventory held at Supplier locations are properly managed, including asset tagging of all End User Devices; e. management of the agreed Standard Operating Environment provided by the Customer; f. imaging/re-imaging/repurposing and deployment of End User Devices and Peripherals including provisioning of Unclassified Loan devices; g. secure issuing of all Devices to Users h. threat and vulnerability management; i. dispatch and delivery of End User Devices and Peripherals direct to Users; j. warranty management for any devices that require return to the original manufacturer or supplier for repair under warranty; and k. Decommissioning, sanitisation and storage of End User Devices and Peripherals, in line with the Customer's Security Requirements, as required; l. liaising with the Customer for removal of stock;		
iii.	Ensure secure storage is provided within a distance that allows transport and reception of End User Devices, Peripherals and associated equipment to and		

from Customer locations within 1 business day, ensuring that the secure storage area shall fulfil all requirements for safe and secure storage areas including related access control and a loading/unloading area		
End User Device Maintenance		
b) provide servicing, maintenance and repair of faulty End User Devices, Peripherals and associated equipment including but not limited to; i. replacement of End User Devices, Peripherals, and associated equipment deployed as part of the Service where the device or Peripheral has been subject to failure attributable to the hardware ii. performing the necessary corrective repairs (where it is cost-effective to do so) and verification tests on End User Devices, Peripherals, and associated equipment, returning repaired devices to the usable spares inventory; iii. repurposing of returned End User Devices, Peripherals and associated equipment for reissue to Users; and iv. management of stock for the replenishment of defective parts (deemed beyond reasonable repair) that require a return to the original manufacturer or supplier for repair or replacement under warranty		
Spares Management		
c) provide a Spares Management function capable of managing the lifecycle of spare Service Assets in the TrIS Service Supply chain, including but not limited to; i. inventory management to maintain appropriate stock levels of usable Service parts, actively managing stock levels in respect of lead times within the supply chain, alerting the customer to any catalogue items that have lead times that could risk service delivery; ii. procurement of spare Service Assets to maintain the levels specified in the spare parts report, providing the Customer with at least 60 Working Days'	The Customer shall own all End User Devices and Peripherals and may request the Supplier to procure End User Devices and End User Device Peripherals, parts or spares, in accordance with the Procurement Service.	

notice (unless otherwise agreed by the SIAM Supplier and/or the Customer) of the procurement requirement		
Vulnerability Management		
d) provide an end-to-end vulnerability management service for the administration and monitoring of information security vulnerabilities across all End User Devices and applicable technology components (e.g., Operating systems, applications, hardware and firmware), including, but not limited to; i. assessing system and software vulnerabilities as soon as they become publicly known (e.g., CERT advisories and subscribing to vulnerability notification services); ii. identifying and obtaining patches (including patch bundles, critical updates and service packs) when they are available to remediate discovered vulnerabilities (e.g., by working with software vendors, or downloading from approved vendor sites); iii. ensuring that anti-malware measures are in place to detect malicious and/or potentially malicious code of any kind as well prevent it from running and remove it from the device; iv. together with the Customer, decide when to deploy patches and analyse the results of testing of the patches as required; and v. responding to antivirus software alerts and perform basic remediation steps as required;	The Customer shall agree with the Supplier when to deploy patches.	
Standard Operating Environment Management		
e) provide management for the ongoing administration, maintenance, and future planning needs of the Customers common Standard Operating Environments including, but not limited to;		Each of the Other Suppliers shall cooperate where relevant in the provision of a new Standard Operating Environment and take all reasonable measures to ensure

i. managing and maintaining and documenting the Standard Operating Environments, in line with the specifications dictated in Annex 2, for all End User Devices to operate with the Customer's cloud-based infrastructure; ii. ensuring that the Standard Operating Environments adhere to the Customer's Security Requirements; iii. ensuring that common Standard Operating Environments are subjected to independent IT Health Checks (penetration testing) carried out under NCSC CHECK terms and conditions; iv. modifying Standard Operating Environment settings as required, agreeing changes to configurations with the SIAM Supplier and Customer; and v. as required, develop new common Standard Operating Environments, liaising with the Customer and the Other Suppliers as appropriate;		the interoperability of all supplier provided software.
Configuration Management		
f) provide management for the ongoing configuration of End User Devices as required including but not limited to; i. ensuring all devices are configured and managed with Standard Operating Environments that meet the requirements outlined in Annex 2; ii. installation and configuration of cryptographic software shall be in accordance with the Customer's Security Requirements; iii. managing capacity to apply Standard Operating Environments to devices at the volume levels required by the Customer; iv. configuration capability (at Supplier location), which allows a Standard Operating Environment, hardened to NCSC guidelines, to be applied on End User Devices prior to delivery;		The SIAM Supplier shall design, provide and manage a comprehensive Release management service to the Customer to plan and co-ordinate the implementation of Releases.

v. ensuring that devices are tested in accordance the Customers Test Policy in Schedule S2 (Testing Procedures) introduced into service in accordance with the Release Management Service;		
Unclassified Load Device Management		
g) provide management for the ongoing administration for all Unclassified Loan Device related activities, including but not limited to; i. managing the complete loan process from initial receipt of an approved Service request through to distribution of device and return of the loaned equipment from the User; ii. on return of the device, ensuring that that the device is reset and rebuilt and that any accounts and data are securely removed from the device as appropriate prior to it returning to the loan pool (unless HMT Security specifies that certain Unclassified Loan Devices be handled differently, such as when a device is temporarily removed from the loan pool to undergo forensic examination);		
Device Deployment		
h) provide deployment and installation of End User Devices, Peripherals, associated equipment and other devices and/or equipment covered by this contract (e.g. Workplace Adjustment equipment) as requested. i. delivery of End User Devices, Peripherals and associated equipment to the User specified by the Customer; ii. configuration and installation of appropriate device drivers and associated monitoring software on End User Devices (e.g. non-networked print devices); iii. configuration, installation, management, and support of mobile service network access devices (such as dongles) and SIMs;		

iv. carrying out any necessary pre-installation checks designed to check the adequacy of the enabling Infrastructure and resolve any issues arising from the pre-installation checks that may impede or delay the installation (Including broadband installation); and v. testing End User Devices, Peripherals, and associated equipment after the appropriate installation to ensure that it is operating correctly in accordance with the testing procedure, in accordance with Schedule S2 (Testing Procedures) i) arrange for secure transportation of End User Devices, Peripherals, and associated equipment between the Suppliers secure storage facility and the location requested by the User recognising that this may not be a Customer Premise including but not limited to; i. delivery of devices to Users; and ii. collection and/or return of devices from Users		
Device Decommissioning		
j) withdraw and decommission End User Devices, Peripherals, and associated equipment when they become obsolescent from an operational and support viewpoint or when otherwise requested by the Customer including but not limited to; i. shutting down, powering off and disconnecting devices from power outlets and the customer's network; ii. disassembling and packing devices using environmentally appropriate packaging materials to ensure they are not damaged in transit; iii. performing quality assured sanitisation and data erasure of devices (including the removal of components, drives and/or magnetic media) in accordance with NCSC guidelines and any specific customer requirements, prior to removing the device from the Customers site;		

iv. updating customer asset registers or configuration management databases; and v. providing a report to the customer setting out decommissioned device asset numbers and the status of that device, for example "missing keyboard"		
VC Equipment Maintenance		
k) Support and maintain Video-Conferencing Equipment and peripherals, including Teams Rooms video-conferencing endpoints and associated screens and peripherals;		
Workplace Adjustment Devices		
l) provision and maintenance of Workplace Adjustments Hardware and Software required to meet the Customer's obligations under health and safety and disability discrimination legislation,		
License Management Support		
m) liaise with the SIAM Supplier who is responsible for License Software Asset Management service and ensure we have licenses available/ on standby by an amount specified by the Customer and procure any licenses where there is a deficit;		
Mobile Device Management		
n) represent the Customer, with delegated responsibility to manage interactions with the Customer's mobile service provider including but not limited to: i. device provisioning; ii. activation of assets; iii. porting of numbers; iv. unlocking devices; v. registering and enrolling devices;		

vi. enabling/disabling international data roaming; vii. reporting lost/stolen devices; viii. managing mobile account cessations;			
2.5 Standards			
a) implement security patches in line with the agreed Release management processes and procedures which shall include, but shall not be limited to the following activities; i. manage and coordinate Release Packages with the Other Suppliers ii. testing of patches and upgrades in compliance with the provisions of the Customers Test Policy in Schedule S2 (Testing Procedures); and iii. rollback patches and upgrades in case of change release failure; b) produce and deliver to the Customer for approval, no less than 30 days before Service Commencement, policies, and processes for the delivery of security patch management			
c) produce and deliver to the Customer for approval, no less than 30 days before Service Commencement, an Asset Register for the traceability of assets owned by the Customer			The SIAM Supplier shall manage and coordinate the Service Asset and Configuration Management Process across the Customer, the Other Suppliers
d) produce and deliver to the Customer for approval, no less than 30 days before Service Commencement, policies, and processes in the area of configuration, in particular quality assurance and configuration;			
e) ensure that End User Device Management at all times effectively interfaces with all other appropriate ITIL processes;			

f) integrate any Supplier tooling for SACM with the Customer's Configuration Management Database (CMDB) in accordance with the Customer's service asset and configuration management policies, processes and procedures;		
g) perform Service Asset and Configuration Management activities for all End User Devices, Peripherals and associated equipment, in accordance with the Service Asset and Configuration Management policies and procedures, including but not limited to; i. establishing and maintaining an Asset Register of End User Devices, Peripherals and associated equipment, and make this available to the Customer; ii. ensuring that End User Devices, Peripherals and associated equipment , are uniquely identifiable to the level of granularity required (including asset goods tagging); iii. ensuring that each End User Devices, Peripherals and associated equipment, is recorded and categorised in the Customers Central CMDB maintaining any changes to End User Devices and owners, including updating the CMDB when Devices are lost and found; iv. keeping full and accurate records of all loans made and make these available to the customer upon request, and on a monthly basis; and v. identifying redundant and/or inactive Assets that are no longer required for the provision of service or no longer capable of being deployed to meet service levels or otherwise not part of the services but owned by the Customer and surplus to the Customer's needs	The Customer Supplier shall implement a Configuration Management database (CMDB) that provides a single view of Service Assets and Configuration Items live on the estate and in line with the Service Asset and Configuration Management process, policies and procedures.	The SIAM Supplier shall monitor the compliance of all Suppliers against the Service Asset and Configuration Management policies and procedures.
h) ensure that discovery and audit tools for the Service are configured to the operational requirements of the Service, Asset and Configuration Management processes, policies and procedures and at all times remain compatible with the customers ITSM Toolset		All of the Other Suppliers shall agree the Service Asset and Configuration Management policies, processes and procedures.

i) provide full details of any tools and methods they reference in their response that are not publicly available methods and standards		
j) ensure all User equipment moving outside of the Customer Premises is handled and stored as required in accordance with Schedule S3 (Security Requirements)		
4. Service Measurement and Reporting		
k) Please refer to Annex 3 (Reports) for all reporting requirements for End User Device Management		

3. Application Management Service

The Application Management function shall provide a variety of application services, processes, and methodologies for controlling, maintaining, and managing custom applications, packaged software applications or cloud delivered applications (such as the O365 suite) throughout their lifecycle. The supplier shall be capable of delivering;

i. configuration, management and deployment of services within the Microsoft 365 environment;
ii. application performance monitoring to measure the end-to-end performance of the Business Applications selected by the Customer;
iii. end-to-end application lifecycle management of Core Applications and Line of Business Applications
iv. recommendations and guidance to facilitate decision making relating to the Customer's hardware and application architecture
v. release management
vi. licence management
vii. identity and access management.

3. Application Management Service		
Supplier Obligations	**Customer Obligations**	**Other Supplier Obligations**
3.1 Outline Provide a comprehensive Application Management function to the Customer to control and maintain a defined set of business software and applications and associated interfaces including but not limited to; • Core Applications • Line of Business Applications • Developed Applications; • Microsoft 365 product suite; and • Directory Services (Active Directory Domain Services and Azure Active Directory);		
3.2 Service Hours		

08:00 to18:00 Monday to Friday (excluding UK bank holidays); and Out of hours cover to respond to escalations (Priority 1 and Priority 2 Incidents) as required		
3.3 Scope • The Core Applications • The Line of Business Applications • The Developed Applications; • Microsoft 365 product suite; • Directory Services (Active Directory Domain Services and Azure Active Directory); • Any other type of application that is added throughout the Contract duration		
3.4 Services Working with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
General Requirements		
a) provide end-to-end Application Lifecycle Management for the Customer's Core and Line of Business Applications, as specified in Annex 2, including but not limited to; i. application packaging to enable deployment of the Customers software applications to End User Devices; ii. software development (where applicable) subject to appropriate controls (i.e., Impact Assessments) to manage exposure and impact (such as cost and resource constraints) as required;		The SIAM Supplier shall design and manage the Licence Software Asset management oversight service. Each of the Other Suppliers shall align its processes with the Licence Software Asset management oversight service to create an end-to-end, seamless and ITIL aligned

iii. management and coordination of Releases into supported environments, including those specified by the TrIS Cloud Platform Services in Annex 2, including scheduling, implementation and post implementation reviews, in line with the Release Management service ; iv. testing and quality assurance in accordance with the testing service in Schedule 2 (Testing Procedures); and v. managing and operating all interfaces between Applications to reasonably maximise application performance, availability, and efficiency; b) proactively monitor the use of all Software to maintain strict compliance, including but not limited to: i. notifying and advising the Customer of any license compliance issues identified within the Customer's Supported Environments or associated with the use of or support of the Services provided to the Customer; ii. providing periodic reporting of license information and compliance to the Customer, in line with the Licence Software Asset Management Oversight Service, as required; and iii. ensuring appropriate monitoring is put in place for the purposes of identifying the presence of any unauthorised, non-standard Software, executables, and other potentially harmful code, in line with the Customer's security policy, unless previously agreed by the Customer Security team c) use appropriate tools to proactively monitor the Customer's application architecture, where relevant, on a continuous basis to prevent or minimise any Service failures and ensure that: i. the monitoring or taking of measurements shall be passive in nature and shall not have any impact on the performance of either the Application being measured or the infrastructure it is accessed through unless otherwise agreed with the Customer;		Licence Software Asset management service.

d) at the request of the Customer, provide information, resources and advice that assists the Customer by undertaking the following: i. recommendation of new tools and COTS software to support or better support Users; ii. reviewing proposed COTS applications and assessing the security impact using criteria from the Customer's own Security team; iii. development and agreement of changes to architecture rules (architecture and technology principles, policies, standards and reference models); iv. development and agreement of changes to the Customer's application architecture (including modification to Applications and associated interfaces), application architecture management and architecture compliance policies, processes and procedures; e) identify and obtain Releases (including Emergency Releases and feature updates) when they are available (e.g., by working with software vendors, or downloading from approved vendor sites) and, where specified, inform the Customer in writing of the impact of implementing each Release; f) carry out and document all housekeeping tasks for the Core Applications and the Line of Business Applications (unless otherwise agreed), including, at the request of the Customer, and where relevant to each application concerned: i. reviewing, acting on and (once the issue has been dealt with) clearing messages; ii. maintaining background tasks; iii. re-routing error workflows; iv. maintaining coding tables; and		

v. ad-hoc running of scripts/agents at the request of the Customer where this does not compromise services; g) manage compliance with all Software licences (including plans in Microsoft 365 as required) by monitoring and auditing all Software use on behalf of the Customer in accordance with the Customer's Licence Software Asset Management policy including but not limited to; i. harvesting any licenses from the dormant accounts, at least monthly, and notify the SIAM Supplier; ii. manage the procurement of all Software licences provided to the Customer on behalf of the Customer and utilise the licences in the most cost-effective manner available; and iii. notifying the SIAM supplier if the procurement of additional licenses (including Microsoft 365) is required. A minimum of five days' notice is required; h) comply with the access limitations that apply to the TrIS Infrastructure, including any requirement to provide install, maintain and support additional software to: i. permit the Supplier to prohibit access to certain types of content in accordance with security policies and as agreed with the Customer; ii. permit the Supplier to allow the capability to make changes to content access policies (either to allow or to prohibit) individually or for a group and as agreed by the Customer; iii. notify the Customer if any item of software is not at least running at n-1 unless agreed by the parties to the contrary.		
Directory Management		
i) provide ownership, management and proactive maintenance of the directory management software (such as Azure cloud, Active Directory or equivalent) systems and services including but not limited to;		A delegated administration model for all directory management software will be agreed with the Customer and Other Suppliers.

i. configuration and maintenance of the Azure Domain Services to work in parallel with the on-premise services and synchronise account information with the Azure AD, on premise AD and SharePoint Online; ii. management of Active Directory Domain Services, including but not limited to Directory Services, DNS, Sites and Services, Domains and Trusts, PKI, third-party SSO integrations and tools; and; iii. management and maintenance of distribution list (including all additions, deletions, and changes) and address books as required. j) provide Access and Identity Management for the Identity and Directory services in accordance with the Customer's Access Management Policies including but not limited to; i. creation and maintenance, including modification, closure, and deletion of domain accounts for Users and their access rights; ii. maintaining a comprehensive register of all Users and Guest accounts and make this register available, upon request, to the SIAM Supplier and/or Customer; iii. creation and maintenance, including modification and deletion, of systems administration accounts and passwords or other authentication credentials; iv. maintaining directories of Users, their details and their access rights to Applications, folders, and data (including that held on Databases); v. perform routine maintenance for the proactive removal of dormant accounts and associated access permissions; vi. manage controlled access to the Customer's third-party suppliers, specified by the Customer, where necessary for the Customer's third party suppliers to provide software support; and vii. granting access to the Active Directory to the Other Suppliers, where appropriate and agreed by the Customer, in order for them to perform administrative functions as required;		

Microsoft 365 Management		
k) monitor the state of the Microsoft Cloud Tenant against the agreed design criteria and notify the Customer as soon as they become aware of any issue or potential issue and provide a proposal for remediation. As a minimum this should include, but not be limited to; i. daily review of Microsoft 365 Admin App; ii. daily review of Microsoft 365 Service Health; iii. daily review the Microsoft 365 Message Centre;		A delegated administration model for the Microsoft Cloud Tenant will be agreed with the Customer and Other Suppliers.

l) provide administration and lifecycle management (including the configuration, management and deployment of services) within the Microsoft 365 product suite of collaboration and productivity tools such as, including, but not limited to; i. Microsoft Exchange; ii. Microsoft Teams, Office Groups, and Office Apps; iii. SharePoint Online (including third-party add-in facilities, and third-party web parts); and iv. OneDrive m) deploy, maintain, and support SharePoint Online based applications (developed by or behalf of the Customer); n) perform records management of Office 365, including developing and deploying controls, support content disposition, and export of records to The National Archive; o) manage the Office Groups lifecycle including, but not limited to: i. enable and apply Retention policies and labels to Office 365 groups, MS Teams and SharePoint sites; ii. Creation of MS Teams and Office 365 groups; iii. Closure of MS Teams; iv. owner/Membership management of MS Teams Office 365 groups to ensure at least two Registered Users as owners for each Team; v. guest access management of MS 365 groups, including MS Teams access, including dormant guest access removal; vi. processing and management of orphaned and dormant User accounts, with removal ultimately approved by the Customer;		The SIAM supplier shall manage the Licence Software Asset Management Oversight Service. SIAM Supplier shall design and provide a comprehensive Security management co-ordination and oversight service

vii. Archival of unused mailboxes connected to the Office 365 group; viii. teams room management; p) maintain, monitor and where possible leverage solutions or guidance to Users via automated means, such as the artificially intelligent 'chatbot' – 'Dot the Bot' – that the Customer has integrated into their MS Teams product q) ensure compliance at all times with the Customer's governance/policies, with a particular focus on document management - sharing, storage and use when accessed via MS products (such as Teams), and include, but not be limited to applying the following categories of control: i. Preventative controls to prevent non-compliance with the Customer's governance/policies particularly with regards Records Management and 'Guest Access' policies applicable to MS Teams; ii. Detective controls to detect and report when an activity, process, or system is out of compliance with the Customer's governance/policies; iii. Directive controls, via policies and 1st Line guidance for example, to enable and drive appropriate behaviour by Registered End Users, e.g. By MS Teams Team owners during the lifecycle of the MS Teams Team that they own that any Information accessed via the Teams Team is compliant with applicable Customer Governance and Policies. r) carry out all housekeeping responsibilities that relate to the Microsoft 365 Productivity Suite in compliance with all applicable Customer governance, policies & processes including, but not limited to; i. lifecycle management of MS 365 groups which covers the creation, archiving and deletion of MS 365 groups, including connected services such as exchange, SharePoint site with/without MS 365 groups, Planner with/without MS 365 groups, MS Teams for MS 365 groups, MS Forms and MS PowerApps;		

ii. ensure appropriate licensing is in place to support data retention requirements for all MS 365 containers, including share mailboxes; iii. apply litigation holds on MS 365 containers, such as MS 365 groups, Teams, mailboxes (including shared mailboxes), SharePoint sites, OneDrives, as directed by the Customer to support court cases and other scenarios as required, and ensure appropriate licensing is in place to support data retention requirements; iv. configure, maintain and update any bridging software or firmware required for all Video Conferencing Equipment, including Teams Rooms video-conferencing endpoints; s) work with SIAM supplier and the Customer to ensure security policies and/or conditional access policies are updated to allow/block external/guest access from authorised and unauthorised domains; t) ensure access to products, services, documents, and applications reflect applicable User profiles and access permissions;		
3.5 Standards		

a) ensure all information pertaining to the Supplier's services is supplied to the SIAM supplier to maintain a dedicated knowledge base for the Customer b) work with SIAM supplier and the Customer to enable federated access between the Customer and other government departments, as directed by the Customer; c) provide access to Services in accordance with the Customer's Access Management Policy d) ensure that all changes to access comply with the Customer's Access Management and Change Management policies, processes and procedures and the SIAM Supplier's Operational Procedures for granting access to Services e) manage and enforce directory standards and group policy objects in accordance with the agreed technical standards, conventions, and protocols f) notify all users of their logon credentials for devices and accounts g) manage and coordinate Release Packages into all Supported Environments (where appropriate and practical, combine Release Packages into a single Release) in accordance with the Part B Release Management policies, processes and procedures. h) test Releases (including those produced by the Customer) in accordance with the testing service in Schedule XX (Testing service); and Paragraph XX (Release management service); i) review and advise the Customer of any Microsoft Office 365 updates, features and changes in line with the Customer's update channel for cloud applications and services that may adversely impact the service;		
3.6 Service Measurement and Reporting		

a) create ad-hoc exports of Users' personal and contact details as directed by the Customer for later import by the Customer, other Government departments or other Customer approved organisations into a mail service global address list or other approved list.		

Service Requirements
Tris2022 Part B - Working with the Other Suppliers

2 Part B – Working with the Customers Other Suppliers

2.1 Service Integration and Management Oversight Service

Service Integration and Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.1..1 Outline The Supplier shall align its processes with the Service Integration and Management Oversight service provided by the SIAM Supplier to create an end-to-end, seamless and ITIL aligned Service Integration and Management Oversight service across the Customer's Services.		The SIAM Supplier shall design and provide a comprehensive Service Integration and Management Oversight Service in respect of the TrIS Services being provided to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.1..2 Scope All Users; All Relevant Services; and All Premises		
2.1..3 Service Hours 08:00 – 18:00 Monday to Friday (excluding UK Bank holidays)		

Service Integration and Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
24 hours a day, 7 days a week, 365/6 days a year during Critical Periods		
2.1..4 Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Processes, Procedures and Collaboration		
a) comply with the Customer's suite of ITIL aligned processes and procedures;		The SIAM Supplier shall establish and implement the suite of ITIL aligned processes and procedures.
b) comply with the Operational Level Agreements (OLAs) agreed with the SIAM Supplier and/or the Customer and the Other Suppliers;		The SIAM Supplier shall establish and implement Operational Level Agreements (OLAs).
c) provide reasonable co-operation, information, documentation, advice and assistance to allow the creation of a comprehensive and consistent suite of standards, policies and services for all aspects of the integration and delivery of the end-to-end Services;		The SIAM Supplier shall establish and implement ways of working, processes and procedures guidance and supporting collaboration guidance for issue to the Other Suppliers. The SIAM Supplier shall establish and implement establish communication channels and collaboration approaches among Other Suppliers to ensure faster turnaround for root cause analysis of Incidents and

Service Integration and Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
		Problems.
d) comply with the communication channels and collaboration approaches to ensure faster turnaround for analysis of Incidents and Problems;		
e) participate in the Service Governance Boards and other governance meetings, in accordance with Schedule 7;		The SIAM Supplier shall design and establish the Boards, in accordance with Schedule S7, and any other governance meetings necessary to provide effective governance, direction and oversight of the Services, and to support the day-to-day management of the Services.
Service Reviews		
f) attend regular (monthly frequency) Service Reviews and on request with no less than 1 weeks' notice, at a Customer designated location and in support of the agreed governance requirements set out in Schedule 7;	The Customer shall attend the service reviews.	Each of the Other Suppliers shall attend the service reviews with the SIAM.
Standards		
g) process, handle and store any data/information directly related to the provision of the Service in full compliance with the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018;		
Reporting		

Service Integration and Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
h) where instructed by the SIAM Supplier and/or Customer, update the information in the Customers Central CMDB in accordance with the Customer process or agreed Service Asset and Configuration Management Policies, Processes and Procedures; i) provide management information and reports to the SIAM Supplier and/or the Customer, including those listed at Annex 3 (Reports);	The Customer shall license, configure and maintain the ITSM tool for the Central CMDB.	The SIAM Supplier shall provide a regular reporting service to the Customer including, collating, reviewing and presenting the Other Suppliers) management information and reports to the Customer.
j) engage with and provide Relevant Services information input into the Reports as instructed by the SIAM Supplier and/or the Customer;		
k) engage with and provide Relevant Services information to allow the Customer to respond to: i) Parliamentary Questions; ii) Freedom of Information (FOIA) requests; iii) Security or Human Resources investigations being undertaken by the Customer insofar as the matter relates to the Services, or consumption of Services by all Users, a group of Registered Users or an individual User;		

2.2 Security Management Oversight Service

Security Management Co-ordination and Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.2..1 Outline The Supplier shall align its processes with the Security management co-ordination and oversight service provided by the SIAM to create an end-to-end, seamless, and ITIL aligned Security management and co-ordination service across the Customer's Services.		The SIAM Supplier shall design and provide a comprehensive Security management co-ordination and oversight service in respect of the Security Alerting Service (or successor service) provided to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer. The Security Alerting Service (or successor service) Supplier shall provide the Security Alerting Service (or successor service) to the Customer.
2.2..2 Service Hours 08:00 – 18:00 Monday to Sunday (excluding UK Bank Holidays) for meetings and reporting		
2.2..3 Scope All Relevant Services		
2.2..4 Services To work with the Customer and the Other Suppliers, the Supplier shall:		
Monitoring		

Security Management Co-ordination and Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
a) receive from the Security Alerting Service (or successor service) any potential Security related incidents, alerts or notifications that have exceeded a predefined threshold from the Security Alerting Service Supplier.		The Security Alerting Service (or successor service) Supplier shall ensure that alerts/notifications generated are fully optimised to minimise possible false positive alerts/notifications The Security Alerting Service (or successor service) Supplier shall ensure the SIAM Supplier and Customer's security personnel have access to all Security Operations Centre alerts/notifications, preferably using a well-designed and easy to view dashboard.
Incident Response		
b) work collaboratively with the Other Suppliers; and respond to and resolve, any Security related Incidents, alerts or notifications within the defined Service Levels;		
Security Incident Remediation		
c) following an agreed Security Incident, participate in a lessons learned review; i) identify the areas for improvement and agree a remediation plan; ii) prioritise the implementation of any resulting actions within the target dates agreed in the remediation plan; and iii) provide regular status updates and attend as required progress meetings with the SIAM Supplier and/or the Customer (to which Other Suppliers may be invited);	The Customer shall agree the frequency of any status updates/progress meetings.	The SIAM Supplier shall undertake and lead a lessons learned review with the Other Suppliers.
Cyber Incident Response		
d) during a Cyber Security Incident (or cyber-attack), work and communicate closely with the Customer personnel and Other Suppliers; and		The SIAM Supplier shall manage and co-ordinate all Incident response activity undertaken.

Security Management Co-ordination and Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
e) support the Customer and any specialist personnel working for any organisation (for example, but not limited to, NCSC or Microsoft) whom the Customer may call upon to help assist with investigating and resolving the incident;		
Operational Security and Security Strategy Meetings		
f) attend monthly operational security meetings; g) where agenda items pertain to the Relevant Services, attend quarterly security strategy meetings;	The Customer shall agree the meeting agendas and attend the monthly operational security meetings and the quarterly security strategy meetings.	The SIAM Supplier shall organise, chair and operate (including a secretariat function) for the monthly operational security and quarterly security strategy meetings.
Security Breach Reporting		
h) on a monthly basis, notify the SIAM Supplier and/or Customer of security breaches relating to the Services including (but not be limited to): i) (where applicable), lost and stolen equipment items including End User Devices; and ii) data losses;		The SIAM Supplier shall on a monthly basis, deliver a consolidated report to the Customer of security breaches relating to all of the TrIS Services.
IT Health Checks/Penetration Testing		
i) actively participate as required in CHECK IT Health Checks (penetration testing) of all components of the TrIS Services for; i) for any newly implemented component; ii) at least annually for any existing already in-service component; iii) and for some major non-routine upgrades (to be agreed with the Customer) of any component; j) review the CHECK IT Health Check (penetration test) reports;	The Customer shall agree the remediation actions as completed.	The SIAM Supplier shall organise and deliver CHECK IT Health Checks (penetration testing) of all components of the TrIS Services via an independent supplier. The SIAM Supplier shall provide copies of the CHECK IT Health Check (penetration test) reports to the Customer and Other Supplier personnel (as relevant) for review.

Security Management Co-ordination and Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
i) work with the SIAM Supplier to create a remediation action plan (in conjunction with the relevant Other Suppliers) setting out how each vulnerability identified in the CHECK IT Health Check (penetration test) will be addressed with target implementation dates; ii) on a fortnightly basis, issue a progress report to the SIAM Supplier and/or the Customer on the remediation plan actions until they have been agreed as completed;		
Reporting		
k) provide security information and reports to the SIAM Supplier and/or the Customer, including those listed at Annex 3 (Reports);		

2.3 TrIS Induction Training Service

TrIS Induction Training Service – NOT APPLICABLE to the Cloud, Infra-structure and Platform Services supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.3..1 Outline The Supplier shall align its processes with the TrIS induction training service provided by the SIAM Supplier to create an end-to-end, seamless and ITIL aligned TrIS induction training service across the Customer's Services.		The SIAM Supplier shall, in collaboration with the Other Suppliers, design an induction training service/course that is tailored to the needs of Registered Users and others, as specified by the Customer.
2.3..2 Scope All new Registered Users Registered Users returning after a period of absence		
2.3..3 Service Hours 24 hours a day, 7 days a week, 365/6 days year - computer based online training (e-learning); 08:00 - 18:00 Monday to Friday (excluding UK Bank Holidays) - 1 to 1 training		
2.3..4 Services To work with the SIAM supplier and the Customer, the Supplier shall:		
Induction Training		
a) support the SIAM Supplier in the design of an induction training course that is tailored to the needs of Registered Users and others, as specified by the Customer which at a minimum shall include: i) logon to the Services;		The SIAM Supplier shall in collaboration with the Other Suppliers, design an induction training course that is tailored to the needs of Registered Users and others, as specified by the Customer.

TrIS Induction Training Service – NOT APPLICABLE to the Cloud, Infra-structure and Platform Services supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
ii) ITSM tool (how to access support, log Calls, purchase peripherals etc); iii) security considerations and security measures; iv) the Customer's Acceptable Use Policy; v) the Registered Users intranet; vi) internet access; vii) Microsoft Teams including desktop video conferencing and online messaging; viii) how to use the calendar and how to manage contacts, tasks and mail; ix) remote access to the services; x) a basic introduction to the broad functionality and means of access to the Customer's electronic document and records system (SharePoint); xi) the Users personal storage folders, including the drives available and how/where to save documents for example filing, personal folders and shortcuts; xii) services provided by the Central Service Desk and how to access them; b) support the SIAM Supplier to deliver any aspects of the induction training that pertain to the Relevant Services e.g. logon to the Services; c) provide information and/or User guides for inclusion as part of the TrIS induction training course and materials and covering the use of Services they provide, and update these in the event of changes to their Services;		The SIAM Supplier shall provide the Customer with a monthly summary of training survey results and recommend improvements.

2.4 Continual Improvement and Innovation Service

Continual Improvement and Innovation service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.4..1 Outline The Supplier shall align its processes with the Continual improvement and innovation service provided by the SIAM Supplier, to create an end-to-end, seamless and ITIL aligned Continual improvement and innovation service across the Customer's Services.		The SIAM Supplier shall design, provide and manage a comprehensive Continual improvement and innovation service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.4..2 Scope All Relevant Services		
2.4..3 Service Hours 08:00 – 18:00 Monday to Friday (excluding UK Bank Holidays)		
2.4..4 Service To work with the SIAM Supplier and the Customer, the Supplier shall:		
Improvements and Innovations		
a) proactively consider and notify the SIAM Supplier and/or the Customer of any possible improvements or innovative ideas to the Services and which demonstrate an under-standing of the Customer's business operations and have been tailored to satisfy the Customer's requirements;		

Continual Improvement and Innovation service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
Continual Improvement and Innovation Management Plan		
b) every six months provide all reasonable information and assistance necessary for the Customer to maintain a continual improvement and innovation plan which describes; i) emerging new and evolving relevant technologies which would improve the Supported Systems and/or the Services which the Customer may wish to adopt; ii) new or proposed improvements to the Services and ITIL processes/procedures; iii) new or potential improvements to the interfaces or integration of the Services which might result in efficiency or productivity gains or in reduction of operational risk; iv) changes in business processes and ways of working that would enable the Services to be delivered at lower costs and/or at greater benefits to the Customer including enabling reductions in the total energy consumed annually in the delivery of Services; v) improvements against identified issues such that the Customer can clearly identify the work and the need; vi) initiatives based on analysis of trend data to improve Service Level achievement; c) on request by the SIAM Supplier and/or the Customer, provide comments on the draft continual improvement and innovation plan;		The SIAM Supplier shall provide the Supplier with a shortlist of areas that it would like the Supplier to consider, in order to assist the Supplier in focusing on areas that are most likely to be accepted by the Customer. The SIAM Supplier shall amend the continual improvement and innovation strategy at a minimum, every twelve months.
Continual improvement and innovation report		
d) on a quarterly basis, provide all reasonable information and assistance necessary for the SIAM Supplier to deliver a continual improvement and innovation report which describes: i) confirmation of the benefits achieved in implementing process improvements in the previous quarter; ii) requests for Commercial Change including Projects, to the extent to which they result from the continual improvement process;		The SIAM Supplier shall on a quarterly basis, prepare and provide to the Customer a continual improvement and innovation report which describes delivered and future Service achievements/benefits/plans, including for the Other Suppliers.

Continual Improvement and Innovation service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
iii) future activity, provide a rolling (continuous) twelve-month, future looking plan, (detailed by each quarter) which will include but is not limited to: • identification of the key themes and areas of service targeted for improvement; • new or potential improvements to the quality or responsiveness of the services; • new or potential improvements to the services, or the manner in which they are provided, which will have a beneficial impact upon the environment; • the targets set for continual improvement; • identification of the reasoning and justification for the proposed improvement(s), including a high-level benefits analysis and impact analysis; • new cost saving opportunities;		
Implementing Improvements and Change Control		
e) if the Customer requests, incorporate and act upon any improvement or innovation identified by the Supplier. The parties shall agree the changes in accordance with Change Control procedures and may agree to share any cost reductions arising as a result of implementing such improvements;		

2.5 Central Service Desk Service

Central Service Desk Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.5..1 Outline The Supplier shall align its processes with the Central service desk service provided by the Central Service Desk Supplier to create an end-to-end, seamless and ITIL aligned Central service desk service across the Customer's Services.		The Central Service Desk Supplier shall provide and manage the day to day operation of the Central Service Desk Management service to the Customer. The SIAM Supplier shall provide comprehensive management and oversight of the Central Service Desk service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.5..2 Scope All Relevant Services		
2.5..3 Service Hours Provide support to all Priority Level 1 and Priority Level 2 Calls 24 hours a day, 7 days a week, and 365/6 days a year, as well as provide support to all Calls during Critical Periods 24 hours a day, 7 days a week, 365/6 days a year Provide support for all Calls other than Priority Level 1 & 2 Calls during the hours 08:00 to 18:00, Monday to Friday (excluding UK Bank Holidays).		
2.5..4 Services		

Central Service Desk Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
To work with the SIAM Supplier, the Customer and the Central Service Desk Supplier, the Supplier shall:		
Operation		
a) comply with the agreed Central Service Desk policies and procedures; b) accept Calls from the Central Service Desk; c) interface to the Customer's ITSM tool either via API (Application Programming Interface) or manually updating the Customer's ITSM tool for the management of Service Events across the Service Delivery Lifecycle (SDLC); d) record the actions being taken to progress and resolve Records which have been referred to them by the Central Service Desk in the Customer's ITSM tool, this includes the activity or fix undertaken that led to resolution. e) support the Central Service Desk Supplier in ascertaining whether a Record relates to the Relevant Services or not; and f) when tasked by the Central Service Desk and/or Customer, investigate, and work collectively and individually as appropriate to resolve Records passed to them by the Central Service Desk relating to the Relevant Services to meet the Service Levels. g) contact the Central Service Desk if it becomes aware of any Incidents and Problems affecting the Service to ensure that the Central Service Desk can maintain a complete and accurate record of all (but not limited to) Incidents, Problems, Service Requests and Complaints; h) receive relevant documentation on Customer's ITSM tool to fulfil their obligations in maintaining Calls assigned to them.	The Customer shall provide, configure, maintain and make available to the Central Service Desk Supplier and all Other Suppliers an ITSM toolset, which will include an Application Programme Interface (API), which Other Suppliers can invoke for the management of Service Events across the Service Delivery Lifecycle (SDLC). The Customer shall license, configure and maintain the ITSM tool to: i) record the time at which the Record was allocated; and	The SIAM Supplier shall govern the Central Service Desk policies and procedures. The Central Service Desk Supplier shall ensure that all Calls are recorded in the Customer's ITSM Toolset using a unique sequential reference and shall provide the management for all related editorial activities. The Central Service Desk Supplier shall ensure that the Central Service Desk follow up and update Users on the status of their Records and ensure that Incidents/Problem/Service Requests and Changes shall be deemed closed only after the User has acknowledged that no further action is required, or the pending closure status window has lapsed.

Central Service Desk Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
	ii) allow the status of Records to be inspected by the Customer and approved Customer representatives (who can inspect any Record) in real time.	
Contact with the Central Service Desk		
i) provide the Central Service Desk with up-to-date contact information for their own service desk (or similar);		
Records		
j) provide timely information to enable the Central Service Desk Call records to be updated, ensuring the language used in the updates is professional.		
Recording Actions		
k) record the actions being taken by it to progress and resolve Records referred to it by the Central Service Desk in the Customer's ITSM tool, this includes the activity or fix undertaken that led to resolution.		
Managing Records		
l) provide reasonable co-operation, information, documentation, advice and assistance to the Central Service Desk and/or Customer in ascertaining whether a Record relates to the Relevant Services or not; m) when tasked by the Central Service Desk and/or Customer, investigate, and work collectively and individually as appropriate to resolve Records passed to them by the Central Service Desk relating to the Relevant Services to meet the Services Levels;		The Central Service Desk Supplier shall assign Records to the Other Suppliers for action as required. It shall track the status of Records periodically until closure, coordinating all activities by working with the Other Suppliers as required, communicating any breach of Service Levels to the SIAM Supplier and

Central Service Desk Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
		the Customer;
n) notify the Central Service Desk, in accordance with the Service Levels, if an Incident or Problem is not the Suppliers responsibility to manage,		
o) provide reasonable co-operation, information, documentation, advice and assistance to the Central Service Desk in resolving Incidents or Problems which are not the Supplier's responsibility to manage as part of the Relevant Services including where these relate to products and services that may need to interface with;		
Advice and Guidance		
p) provide reasonable assistance and information to enable the development of a suite of User advice and guidance and Service Knowledge Management System in respect of the Services for inclusion in the advice and guidance knowledge centre.		

2.6 Incident Management Service

Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.6..1 Outline The Supplier shall align its Incident management processes to the Incident management service provided by the Central Service Desk to create an end-to-end, seamless and ITIL aligned Incident management service across the Customer's Services.		The Central Service Desk Supplier shall provide and operate the central Incident Management service for the Customer. The overall purpose of the Incident management service shall be to resolve Incidents with the minimum amount of disruption to the Customer, and in line with the agreed Service Levels. The SIAM Supplier shall design and provide management oversight of the end to end Incident Management service for the Customer. This includes, as necessary, directing the Other Suppliers.
2.6..2 Scope Any Incident assigned to the Supplier by the Central Service Desk		
2.6..3 Service Hours Provide support to all Priority Level 1 and Priority Level 2 Calls 24 hours a day, 7 days a week, and 365/6 days a year, as well as provide support to all Calls during Critical Periods 24 hours a day, 7 days a week, 365/6 days a year. Provide support for all Calls other than Priority Level 1 & 2 Calls during the hours 08:00 to 18:00, Monday to Friday (excluding UK Bank Holidays).		

Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.6..4 Services To work with the Central Service Desk Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Support Team		
a) provide personnel and resolve the Incident if possible;		
Stop Clock		
b) not put any Priority Level 1 Call into "pending" without the agreement of the SIAM Supplier and/or the Customer and not suspend or give other Calls a "pending" status unless or until: i) agreement of the Customer; ii) the User or the Customer has requested the Supplier in writing to put the Call into "pending"; or iii) additional information required from User; c) where it requires additional information from a User in order to be able to progress the resolution of the Call, the Supplier has: i) called the User and left a voicemail message; and ii) sent an email to the correct email address of the User requesting the User to call the Central Service Desk explaining that the Central Service desk needs additional information to deal with the Call; and iii) unless agreed otherwise, notified the SIAM Supplier and/or the Customer; d) where it requires information or assistance from one of the Other Suppliers in order to be able to progress the resolution of the Call, the Supplier has:		Each of the Other Suppliers shall, on request by the Supplier, respond in a timely manner to requests for information or assistance from the Supplier.

Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
i) ascertained who is the correct person to speak to at the Other Supplier; and ii) called the correct person at the Other Supplier and left a voicemail message; and iii) if the person at the Other Supplier has not responded, sent an email to the correct email address of the person at the Other Supplier requesting them to call the Supplier and explaining they urgently needs additional information to deal with a Call relating to the Customer and (for Priority Level 2 Calls) copied the Customer in on the email; and iv) if the Other Supplier has not responded or has responded but has not provided the additional information or assistance, chased the Other Supplier for the additional information or assistance;		
e) promptly inform the Central Service Desk of any Incidents which affect data integrity;		
f) if the cause of the Incident is unknown, refer it to the Problem management team; g) For the sake of clarity, Calls will not be removed from live Incident stack when they are referred to the Problem management service.		
h) if the resolution of the Incident requires a Change, refer it to the Change procedure;		

2.7 Major Incident Management Service

Major Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.7..1 Outline The Supplier shall align its processes with the Major Incident management service provided by the SIAM Supplier to create an end-to-end, seamless and ITIL aligned Major Incident management service across the Customer's Services. The overall purpose of the Major Incident management service is to manage the resolution of Major Incidents affecting or believed to be affecting the Confidentiality, Integrity or Availability of Data, Information or Services, and to restore Service operation, in the event of any Service failure, as quickly as possible with the minimum amount of disruption to the Customer, and in line with the agreed Service Levels.		The SIAM Supplier shall design and provide the Major Incident management service to the Customer. This includes, as necessary, directing the Other Suppliers to resolve Major Incidents affecting or believed to be affecting the Services, on behalf of the Customer.
2.7..2 Scope All Major Incidents (including Major Cyber Incidents) or events relating to the Services		
2.7..3 Service Hours 24 hours a day, 7 days a week, 365/6 days a year		
2.7..4 Service To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		

Major Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
Notification		
a) notify the Central Desk in accordance with the Service Level when a Major Incident or Event has occurred which may impact the Relevant Services;		
b) comply with the SIAM Supplier's processes and procedures for maintaining Records of Major Incidents;		
c) where applicable, provide the SIAM Supplier and/or the Customer, with an initial update on each Major Incident in accordance with the applicable Service Level detailing: i) the action being taken by the Supplier to deal with the major incident; ii) the anticipated time to resolve the major incident; d) where applicable, provide written confirmation when the Major Incident has been resolved; i) start and end time; ii) Priority Level; iii) affected Users; iv) summary of steps taken to resolve the Major Incident; v) root cause;		

Major Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
vi) any corrective actions undertaken or required to prevent re-occurrence;		
Summary Action		
e) provide the SIAM Supplier and/or the Customer with a detailed update on each Major Incident in accordance with the Major Incident Management process		The SIAM Supplier shall ensure that Major Incident reviews are conducted, and the Major Incident report is sent to the Authority within 10 Working Days of the Major Incident being reported to the Central Service Desk.
Incident Re-Prioritisation		
f) reprioritise any incidents re-designated as Major Incidents by the SIAM Supplier and/or the Customer;	The Customer shall promptly notify the Supplier of such re-designations.	
Disaster Recovery/Business Continuity Incident		
g) ensure the Services are brought back into an operational state in line with the Service Levels;		The SIAM Supplier shall manage and co-ordinate all response activity in relation to a Disaster Recovery/Business Continuity Incident. The SIAM Supplier shall define areas of responsibility for the Other Suppliers in respect of their Relevant Services in relation to

Major Incident Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
		a Disaster Recovery/Business Continuity Incident

2.8 Problem Management Oversight Service

Problem Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.8..1 Outline The Supplier shall align its processes with the Problem management oversight service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Problem management oversight service across the Customer's Services.		The SIAM Supplier shall design, provide and manage the Problem management oversight service to the Customer. This includes, as necessary, directing the Other Suppliers to resolve Problems affecting or believed to be affecting the Services, on behalf of the Customer.
2.8..2 Scope All Problems relating to the Relevant Services All Problems relating to the Relevant Infrastructure		
2.8..3 Service Hours 08:00 – 18:00 Monday to Friday (excluding UK Bank Holidays)		

Problem Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.8..4 Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Service		
a) resolve Problems affecting the Relevant Services including to: i) identify the root cause of problems (Root Cause Analysis or RCA); ii) resolve the root cause of Problems; iii) through the term, continually reduce the number of repeat incidents generated in accordance with the Service Levels; iv) use all reasonable endeavours to minimise the adverse impact of incidents and problems on the Customer; v) Prevent the re-occurrence of incidents related to these problems with the Supplier (where necessary) raising a change request;		
Problem Management Team		
b) provide personnel capable of the identification and resolution of Problems;		
c) ensure that the personnel involved in Incident management update relevant information such as Known Errors in the Customer's ITSM tool;	The Customer shall license, configure and maintain the ITSM tool.	
Processes and Co-operation		
d) co-operate with the SIAM Supplier and the Other Suppliers to resolve Problems affecting the Other Services;		
Proactive Problem Management		
e) highlight groups of Users or applications that are experiencing common Incidents and therefore identify Problems;		
f) carry out trend analysis for the Relevant Services, to proactively identify and resolve Problems before Incidents occur;		

Problem Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
Reactive Problem Management		
g) generate Problem requests for recurring Incidents or single Incidents or a set of Incidents where the root cause was unknown at the time of the service recovery or Incident closure;		
h) prioritise Problems by agreement with the SIAM Supplier and/or the Customer based on: i) the priority level of the related Incidents; ii) the number of Incidents relating to the Problem;		
identify workarounds for Problems;		
i) analyse incidents and determine the root cause of the Incidents, ensuring that actions for improvement have been identified during the Problem management process are recorded and put into plans for improving the Relevant Services;		
j) manage and resolve the root cause of those Incidents relating to the Relevant Services, to ensure that Problems relating to the Services are resolved as quickly as possible, in line with Service Levels		
Provision of Information		
k) notify the SIAM Supplier and/or the Customer of Known Errors and Problem resolution affecting its Relevant Services;		
l) deliver to the SIAM Supplier and/or the Customer a report fully detailing the root cause of the Problem together with any remedial actions taken or required with a plan to implement such remedial actions;		
Change		
m) if the Problem requires a Change, refer it to the relevant procedure (Change management service);		

Problem Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
n) if the resolution of the Problem necessarily requires the Customer to procure additional hardware and software for which it is responsible, refer the Problem to the Change Control Procedure;		
Review Meetings		
o) attend monthly Problem review meetings with the SIAM Supplier and/or the Customer;		

2.9 Communications, Advice and Guidance Service

Communications, Advice and Guidance Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.9..1 Outline The Supplier shall align its processes with the Communications advice and guidance Service provided by the SIAM Supplier, to create an end-to-end, seamless and ITIL aligned Communications, advice and guidance service across the Customer's Services.		The SIAM Supplier shall design and manage a comprehensive Communications advice and guidance service for the communications required with the Customer, Other Suppliers and with Users, where Users need to receive information relating to the Services including the Other Services.
2.9..2 Scope		

Communications, Advice and Guidance Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
All Services All Users (or a specific category of Users as specified by the Customer) All situations where the Customer or Users need to receive information relating to the Services All reasonable advice and guidance to Users on how to use End User Devices, End User Device Peripherals, Applications and Services		
2.9..3 Service Hours 24 hours a day, 7 days a week, 365/6 days year for communications services in relation to Major Incidents or events relating to the Services 08:00 – 18:00 Monday to Friday (excluding UK Bank Holidays) for all other communications services		
2.9..4 Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Advice and Guidance Provision		
a) provide reasonable assistance and information to enable the development of a suite of User advice and guidance and knowledge base articles in respect of the Services for inclusion in the advice and guidance knowledge centre, including at a minimum; i) where applicable, advice and guidance for Users on how to interact with and/or use End User Devices, End User Device Peripherals, Applications and the Services;	The Customer shall review and provide feedback on the User advice and guidance.	The SIAM Supplier shall, in collaboration with the Other Suppliers, design, produce and manage a comprehensive and consistent suite of User advice and guidance in respect of the

Communications, Advice and Guidance Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
ii) a list of FAQs (frequently asked questions) and answers; **Note** – Advice and Guidance will only be provided for Customer provided End User Devices and End User Device Peripherals, although best endeavours will be made by the Supplier and the Other Suppliers for those not purchased by the Customer. b) provide reasonable assistance to the SIAM Supplier to enable the creation of monthly communications suitable for issue to Users covering general advice, hints and tips, service news, and planned maintenance as agreed; c) provide information to allow for the publication of Services communications including: i) daily Services status updates ensuring Users are notified of any issues affecting availability or usage of the Services; ii) Major Incidents or events relating to the Relevant Services; iii) forthcoming agreed changes or maintenance work relating to the Relevant Services; iv) the introduction of new Services; d) ensure the knowledge base articles are regularly (at a minimum quarterly) reviewed and updated to provide updated information for the advice and guidance knowledge centre or other communications;	The Customer shall provide the make/models information of the provided End User Devices and End User Device Peripherals.	Services to be maintained in an advice and guidance knowledge centre. The SIAM Supplier shall develop and publish a monthly newsletter covering general advice, hints and tips, service news, and planned maintenance. The SIAM Supplier shall develop, maintain and arrange for the publication of regular Services communications including: • status updates for the Services ensuring Users are notified of any issues affecting availability or usability of the Services; • Major Incidents or events relating to the Services; • forthcoming agreed changes or maintenance work relating to the Services; • the introduction of new Services.
Updating the guidance		
e) on a quarterly basis:		

Communications, Advice and Guidance Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
i) review with the SIAM Supplier amendments or additions required to the advice and guidance knowledge centre or other communications; ii) implement agreed changes;		

2.10 Service Catalogue Service

Service Catalogue Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.10..1Outline The Supplier shall align its processes with the Service Catalogue Service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Service Catalogue Service across the Customer's Services.	The Customer shall provide an ITSM platform for delivery of the Service Catalogue.	The SIAM Supplier shall design, manage and make available, a comprehensive, on-line Service Catalogue service for the Customer to allow Registered Users to order items or request ICT goods and services. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.10..2Scope Goods or Services relating to the Relevant Services and the Relevant Infrastructure		
2.10..3Service Hours 24 hours a day, 7 days a week, 365/6 days a year availability of the online Service Catalogue	The Customer is responsible for the availability of the Service	

Service Catalogue Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
08:00-18:00 Monday to Friday (excluding UK Bank Holidays) for all other aspects of the Service Catalogue service	Catalogue.	
2.10..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Service Catalogue Information		
a) provide information relating to the Goods and Relevant Services including price and fulfilment time to be provided by it for inclusion in the Customer's Service Catalogue;	The Customer shall agree which items will be included in the Service Catalogue, the price and the fulfilment time.	
b) provide any other assistance necessary to permit the SIAM Supplier and/or Customer to produce the Service Catalogue;		
c) at least Quarterly, propose changes and provide updated information relating to the Goods and Relevant Services to be provided; i) recommend the inclusion of new/additional or removal of Service Catalogue items and provide any other assistance necessary to update the Service Catalogue;	The Customer shall agree the updated information to go in the Service Catalogue.	The SIAM Supplier shall maintain and update the Service Catalogue.
Provision of Goods and Services		
d) provide relevant Goods and Services ordered by Users from the Service Catalogue in accordance with the terms of the agreement between it and the Customer;		
e) maintain appropriate space for the secure storage of Goods described in the Service Catalogue;		
f) where applicable, maintain a database of excess stock of End User Devices and End User Device Peripherals owned by the Customer for redeployment within the Customer;		

Service Catalogue Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
g) where applicable, identify orders from the Service Catalogue that can be satisfied by the redeployment of End User Devices and End User Device Peripherals held by the Supplier;		
h) provide all other Goods and Services ordered from the Service Catalogue in accordance with the Service Levels;		
Compliance		
i) ensure that all the items in the Service Catalogue comply with the requirements of its agreement with the Customer, including the standards and policies specified in the agreement;		
Benchmarking		
j) at least Annually, participate in a benchmark the Service Catalogue prices to determine if they align with market prices as well as those prices and services available elsewhere to the Customer;		The SIAM Supplier shall benchmark the Service Catalogue prices to determine if they align with market prices.

2.11 Risk Management Service

Risk Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.11..1Outline The Supplier shall align its processes with the Risk management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Risk management service across the Customer's Services.		The SIAM Supplier shall design, provide and manage a comprehensive Risk management service to the Customer. This includes, as necessary, directing

Risk Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
		the Other Suppliers on behalf of the Customer.
2.11..2Scope All risks affecting the Relevant Services All risks affecting the Relevant Infrastructure		
2.11..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays)		
2.11..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Risk Procedures Statement		
a) at the beginning of each Contract Year, provide a letter to the Customer from its managing director (or equivalent) attesting to the fact that, having made due and careful enquiries during the preceding period, the Supplier is confident that its security and risk mitigation procedures, with respect to the Service, remain effective or pointing out any recommendations which the Supplier has made to the Customer which the Customer has unreasonably refused to implement;		
Notification (Early Warning)		
b) notify the SIAM Supplier and/or the Customer of any risk or issue (together with all supporting information available to the Supplier relating to the identified risk or issue) if a risk or issue arises that has (or may): i) result in the Customer incurring any additional or increased costs or expenses; ii) adversely affect the progress or performance of the Relevant Services; iii) delay the successful completion of the tests relating to any Deliverable by the Planned Operational Services Commencement Date or Milestone Date;		

Risk Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
iv) otherwise result in a delay in the performance of obligations relating to the Implementation Services or the implementation of any new Projects; v) impair the Customer's ability to use the Relevant Infrastructure or otherwise adversely affect the Customer's business operations; vi) lead to a Supplier Default or likely Supplier Default; or vii) lead to a Customer Cause or likely Customer Cause;		
Mitigation of Risk		
c) resolve or, if full resolution is not possible, mitigate any risks or issues relating to the provision of the Services agreed as being the Supplier's responsibility in the Risk Register;	The Customer shall act reasonably in resolving or mitigating any risks or issues identified as being the Customer's responsibility in the Risk Register.	The SIAM supplier shall produce and maintain a consolidated Risk Register identifying risks relating to the TrIS Services and any TrIS Projects being carried out by the Supplier or the Other Suppliers, including operational risks and Project risks.
Risk Register		
d) issue to the SIAM Supplier and/or the Customer, on a monthly basis, an accurate risk register that identifies, in so far as is possible, all risks relating to the Services and any Projects being carried out by the Supplier for the Customer, including operational risks and project risks, and that describes: i) the risk; ii) the risk owner, responsible for monitoring risk and tracking the risk mitigation actions; iii) the timing / time when the risk might materialise; iv) the likelihood of the risk occurring; v) the potential impact of the risk from a Service/Project delivery perspective, from an operational/technical perspective and from a financial perspective for the Customer;		

Risk Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
vi) any actions which need to be taken to avoid or mitigate the risk or the impact or the likelihood of the risk; vii) the resources (including financial resources) required to avoid or mitigate the risk; viii) which of the parties is to take the actions to avoid or mitigate the risk or the impact or the likelihood of the risk (this is not necessarily the risk owner); ix) an action plan explaining when the party is to take the actions; and x) the resulting risk, impact and likelihood post-mitigation; e) attend risk reduction meetings (at the monthly review meetings, or on ad-hoc basis as necessary) or at the SIAM Supplier and/or Customer's request;		
Updates to The Risk Register		
f) provide, on request by the SIAM Supplier and/or the Customer, an accurate update on the status and progress of all risk/issue management or mitigation steps that are being taken;	The Customer will review, within 20 Working Days, each new action added to the Risk Register by the Supplier.	

2.12 Service Asset Configuration Management Oversight Service

Service Asset and Configuration Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.12..1Outline The Supplier shall align its processes with the Service Asset and Configuration management oversight service provided by the SIAM Supplier so as to create an		The SIAM Supplier shall design, provide and manage the Service Asset and Configuration Management Oversight service to the Customer to

Service Asset and Configuration Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
end-to-end, seamless and ITIL aligned Configuration management service across the Customer's Services.		identify and account for service assets and Configuration Items, protecting and ensuring their integrity across their lifecycle. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.12..2Scope All Configuration Items relating to the Relevant Services All Configuration Items relating to the Relevant Infrastructure		
2.12..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.12..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Configuration Management		
a) ensure their configuration control procedures maintain the integrity of systems, Relevant Services and service components, including the tagging of physical items of equipment; b) ensure that where changes to systems, Relevant Services and service components are made, all necessary changes are made to related systems, services and service components; c) ensure a baseline of the appropriate Configuration Items is taken before they are Released to the production (live) environment;	The Customer shall license, configure and maintain the ITSM tool for the Central CMDB.	

Service Asset and Configuration Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
d) ensure that master copies of digital Configuration Items are controlled in secure physical or electronic libraries and referenced to the configuration records, e.g. software, testing products, support documents, Release packages, installation scripts and documentation; e) identify on the Central CMDB exactly which Users are affected by Incidents that affect specific Configuration Items (e.g. servers, locations, applications);		
End User Device Configurations		
f) Each of the Other Suppliers shall, during the implementation and onboarding process, provide the EUC supplier with full details of any software or software functionality that they require, and shall notify the EUC supplier of any subsequent changes to their software or software functionality. Any such changes will need to be managed in accordance with the Change Control Procedure. g) Each of the Other Suppliers shall cooperate where relevant in the provision of a new Standard Operating Environment and take all reasonable measures to ensure the interoperability of all supplier provided software.		
Providing CMDB information to the Customers Central CMDB		
h) in accordance with the Customer process, update the information in the Customer's Central CMDB to provide the Customer with a single and complete real-time view of the configuration of the processes and procedures and standards, technology, equipment, hardware and software used by the Supplier to deliver the Relevant Services;	The Customer shall license, configure and maintain the ITSM tool for the Central CMDB.	
Verifying the Suppliers CMDB		
i) ensure that the CMDB is actively managed and verified to ensure its reliability and accuracy: i) carry out local spot checks to determine if any (and if so which) unauthorised changes have been made to installed equipment, and to ascertain any gaps between the actual equipment and its configuration and that maintained by the Supplier in the Suppliers CMDB;		The SIAM Supplier shall maintain oversight of the Central CMDB ensuring it provides a single and complete view of the configuration of the processes and procedures and standards, technology, equipment,

Service Asset and Configuration Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
ii) carry out a regular audit of the accuracy of the Suppliers CMDB in accordance with the Service Levels, maintain records of the results of the audit and make the records available to the SIAM Supplier or the Customer upon request; j) on request by the SIAM Supplier and/or the Customer, correct the Suppliers CMDB if it is incorrect;		hardware and software used by the Suppliers to deliver the Services.
CMDB Updates		
k) update the records on the Suppliers CMDB following any relevant Commercial Changes or Changes which are known to the Supplier, including those resulting from installations, moves, adds, changes or deletions; l) ensure the updates are reflected in the Customer's Central CMDB to avoid the Central Service Desk having to ask the Users unnecessary questions e.g. device asset number when they are logging a Call or providing User support and to ensure the SIAM Supplier and/or the Customer have access to relevant information to avoid them having to ask unnecessary questions e.g. when collating a report.		
Access to the Suppliers CMDB		
m) provide, at any time, authorised representatives of the Customer with read only access to the Suppliers CMDB, including for the purposes of allowing the SIAM and/or the Customer to carry out an audit of the CMDB; and n) ensure that the Suppliers CMDB has multiple filtering and drill-down capabilities which shall be enabled for authorised representatives of the Customer;	The Customer shall license, configure and maintain the ITSM tool for the Central CMDB.	

2.13 Licence Software Asset Management Oversight Service

Licence Software Asset Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.13..1Outline The Supplier shall align its processes with the Licence Software Asset management oversight service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Licence Software Asset management service across the Customer's Services		The SIAM Supplier shall design and manage the Licence Software Asset management oversight service to the Customer to identify and account for the Customer licensed software. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.13..2Scope All Customer Provided Software		
2.13..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays)		
2.13..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Licence Management		
a) on a monthly basis, advise the SIAM Supplier and/or the Customer of the situation re-garding the usage of Customer supplied licences, and any Customer provided licences required but not issued and any changes to that situation. b) advise the SIAM Supplier of any risks to the Customer and which the Supplier is or should be reasonably aware of, which indicate the Customer could face a claim or legal	The Customer shall notify the Supplier of the numbers and types of licences taken out by it with regard to the	

Licence Software Asset Management Oversight Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
action for a breach of its software licence obligations for any items of Customer Provided Software; c) ensure software licences are harvested in a timely manner when a: i) Registered User leaves; ii) Registered User no longer requires the software; iii) Registered User has not used the software for an agreed period of time;	Customer Provided Software.	

2.14 Change Management Service

Change Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.14..1Outline The Supplier shall align its processes with the Change management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Change management service across the Customer's Services.		The SIAM Supplier shall design and provide a comprehensive Change management service in respect of all changes to the provided Services or Infrastructure to ensure the integrity of the provided Services or Infrastructure is maintained. This includes, as necessary, directing the Other Suppliers on behalf of the Customer. The SIAM Supplier shall design and implement change management guidelines and standards and agree them with the Customer.
2.14..2Scope All Changes relating to the Relevant Services All Changes relating to the Relevant Infrastructure		
2.14..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays)		
2.14..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Change Advisory Board (CAB)		

Change Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
a) participate at relevant CAB weekly meetings and emergency (ad-hoc) CAB meetings to discuss proposed relevant upcoming Changes to the Infrastructure;	The Customer shall participate at meetings of the Change Advisory Board to discuss and approve proposed upcoming Changes.	
Impact Change Assessments		
b) provide all necessary reasonable information to enable the preparation of Impact Assessments advising if a proposed Change poses a risk to the Infrastructure or shall have any other impact upon the Customer's business; c) acknowledges and takes full account of the fact that the nature of the Customer's business may necessitate change freezes being instigated by the Customer from time to time including immediately prior to Critical Periods;		The SIAM Supplier shall inform the Other Supplier of change freeze periods.

2.15 Release Management Service

Release Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.15..1Outline The Supplier shall align its processes with the Release management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Release management service across the Customer's Services.		The SIAM Supplier shall design, provide and manage a comprehensive Release management service to the Customer to plan and co-ordinate the implementation of all Changes. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.15..2Scope All Releases relating to the Relevant Services including all Changes All Releases relating to the Relevant infrastructure including all Changes All service documentation		
2.15..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.15..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Complying with Release management policy		
a) agree the Customer's Release Management policy;		The SIAM Supplier shall document and agree the Release

Release Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
b) operate in accordance with the agreed Release management process and Release management policy; c) ensure it does not make any changes to the Relevant Services or Relevant Infrastructure without following the Release management policy and processes;		Management policy with the Other Suppliers.
Impact of Releases on Users		
d) assess the likely impact of the Release on the affected Users and shall: i) advise the SIAM Supplier and/or Customer of that impact, particularly response times to keystrokes and other command actions; and ii) any further mitigations which may be possible to reduce any adverse impacts and any consequences of such mitigations;		The SIAM Supplier shall, as part of the approval of any Release, determine the impact of each Release on Users, and shall not authorise any Release if they believe the Release will have an adverse, unacceptable, and likely to be evident, impact on the performance of the Services provided to Users.

2.16 Scheduled Maintenance Service

Scheduled Maintenance Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.16..1Outline The Supplier shall align its processes with the Scheduled Maintenance service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Scheduled Maintenance management service across the Customer's Services.		The SIAM Supplier shall design, provide and manage the Scheduled Maintenance service to the Customer to: • ensure that there shall be no Scheduled Outages during Core Hours; and • ensure that the backup process shall have no detrimental effect on any service response times and performance perceived by Registered Users and no detrimental effect on the Service Levels. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.16..2Scope All Scheduled Maintenance relating to the Relevant Services All Scheduled Maintenance relating to the Relevant Infrastructure		
2.16..3Service Hours		

Scheduled Maintenance Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.16..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Scheduled Maintenance Plan		
a) provide the SIAM Supplier and/or the Customer with a general, rolling 12 monthly Scheduled Maintenance plan that covers its Relevant Services and takes into account key business periods and events which shall specify; i) the Scheduled Maintenance the wish to carry out to the Infrastructure over the following 12 months; and ii) when the Supplier proposes carrying out the Scheduled Maintenance; iii) provide the plan within one Working Day of the end of each month; b) maintain a controlled copy of its Scheduled Maintenance plan and make it available to the Customer at all times online; c) discuss proposed changes to its Scheduled Maintenance plan at each monthly service review or CAB meeting and agree the changes; d) forward Scheduled Outage requests to the SIAM Supplier and/or the Customer;		The SIAM Supplier shall review and agree the Scheduled Maintenance plan. The SIAM Supplier shall review and agree changes to the Scheduled Maintenance plan. The SIAM Supplier shall notify the Other Supplier of change freeze periods.

Scheduled Maintenance Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
e) acknowledge that the nature of the Customer's business may necessitate change freezes being instigated by the Customer from time to time for business operational reasons;		
Managing the Scheduled Maintenance		
f) carry out the Scheduled Maintenance in accordance with the agreed scheduled maintenance plan and not carry out any Scheduled Maintenance other than as specified in the agreed Scheduled Maintenance plan; g) manage and co-ordinate implementation including full testing and technical systems integration as may be required; i) monitor and report on the implementation;		
Updating The CMDB		
h) ensure its CMDB is updated with all changes made by it as a result of the Scheduled Maintenance;		

2.17 Emergency Outages Service

Emergency Outages Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.17..1Outline The Supplier shall align its processes with the Emergency Outages service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Emergency Outages service across the Customer's Services.		The SIAM Supplier shall design, provide and manage the Emergency Outages service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.17..2Scope Under emergency conditions, the Supplier or Other Suppliers may have to interrupt the Relevant Services (or a component thereof) at short notice. In this situation, the Supplier shall comply with the provisions below. All unplanned outages affecting the Relevant Services		
2.17..3Service Hours 24 hours a day, 7 days a week, 365/6 days a year		
2.17..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Operation		

Emergency Outages Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
a) immediately inform the SIAM Supplier and/or Customer of the requirement for an emergency outage;	The Customer shall review and agree a contact process for use during an Emergency Outage situation.	
Consent		
b) use all reasonable endeavours to obtain the SIAM Supplier consent prior to interrupting the Other Services (or a component thereof), including: i) contacting the SIAM Supplier's Service Manager or other representative; and ii) invoking the escalation mechanism in the event the SIAM Supplier's Service Manager cannot be contacted;		
Proceeding Without Consent		
c) where the Supplier cannot contact the SIAM Supplier to obtain the Customer's consent, proceed with the emergency outage only if the delay caused by seeking agreement shall cause undue damage to the Customer's business, in which case it shall carry out the emergency outage at a suitable time, taking into account the usage of the relevant part of the Relevant Infrastructure and the urgency of carrying out the emergency outage;		
User Communications		
d) assist the SIAM Supplier as appropriate to ensure all Registered Users are informed insofar as the Relevant Services are affected by or the cause of the emergency outage; e)		
Documentation		
f) as part of the configuration management service, complete all retrospective documentation relating to the Fast-Track Change Request		
Service Levels		

Emergency Outages Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
g) be aware, for the avoidance of doubt, any emergency outage shall count towards unavailability for the purposes of the Service Levels;		

2.18 Availability and Capacity Management Service

Availability and Capacity Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.18..1Outline The Supplier shall align its processes with the Availability and Capacity management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Availability and Capacity management service across the Customer's Services.		The SIAM Supplier shall design, provide and manage a comprehensive Availability and Capacity management service to the Customer to ensure that the availability and capacity of the Infrastructure and Services meet the Customer Requirement. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.18..2Scope All Relevant Infrastructure All Supported Environments		
2.18..3Service Hours 24 hours a day, 7 days a week, 365/6 days a year		

Availability and Capacity Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.18..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Capacity Plan		
a) on a monthly basis, provide a capacity management plan with a forecast of the capacity requirements of the Relevant Services or Relevant Infrastructure for the following 12 months to ensure that the capacity meets the Customer Requirements; and i) make available the capacity management plan to the SIAM Supplier and/or the Customer; as part of the monthly service review, b) take all reasonable actions to optimise the availability, capacity and performance of the individual component parts of the Relevant Services or Relevant Infrastructure provided that the ability to correct the same is within the reasonable control of the Supplier, including: i) identifying, defining and agreeing with the Customer any mitigating actions to be taken when capacity thresholds are being approached;		
Monitoring, measurement and analysis		
c) where applicable, use appropriate tools to proactively monitor the Relevant Infrastructure (including processing capability, memory, and bandwidth) on a continuous basis to prevent or minimise the effect of any Relevant Service failure. The Supplier shall ensure that the monitoring tools do not unduly impact on performance or capacity of the Relevant Infrastructure including; i) availability including reliability, maintainability and performance, of the Relevant Infrastructure; ii) analyse the measurement data, including analysing performance and the impact of changes to the Relevant Services; iii) analyse and understand the capacity demands of the component parts of the Relevant Infrastructure;		.

Availability and Capacity Management Service - NOT APPLICABLE to the Central Service Desk Supplier		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
d) provide access for the SIAM Supplier and/or the Customer to the Supplier's monitoring system so that they can see (through a real-time dashboard RAG (red, amber, green) approach) the extent to which Relevant Services (unless agreed by the parties to the contrary): i) are available or not; or ii) are experiencing material degradation;		

2.19 Sustainability Service

Sustainability Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.19..1Outline The Supplier shall align its processes with the Sustainability Service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Sustainability Service across the Customer's Services.		The Supplier shall design and provide a comprehensive Sustainability service to the Customer. The Supplier shall liaise with Other Suppliers to obtain the information needed to provide the consolidated Sustainability service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.19..2Scope All Relevant Services		

Sustainability Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
All Relevant Infrastructure		
2.19..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.19..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Standards and Lifecyle		
a) hold, and provide evidence of holding to the SIAM and/or the Customer, ISO 14001:2015 (or successor) certifications, and operate an environmental management system designed to ensure that all delivery processes, outputs and service delivery mechanisms comply with ISO14001:2015 (or successor) requirements; b) prepare within 180 days of Service Commencement Date and update at least annually, a road map and action plan demonstrating how they will: i) achieve business rules 1-3 of the UK Greening government: ICT and digital services strategy (2020-2025 or successor; ii) support the Customer to achieve the targets in the Sustainable ICT and digital services strategy: targets for 2020-2025 (or successor); and iii) issue the roadmap and action plan to the SIAM and/or the Customer; c) prior to procurement on behalf of the Customer establish that Services or Goods meet the UK Government Buying Standards and requirements under the UK Greening government: ICT and digital services strategy (2020-2025 or successor); d) work to reduce the overall carbon footprint of the Services in line with the agreed target and timeline;	The Customer shall provide the targets from the Sustainable ICT and digital services strategy. The Customer shall agree the carbon footprint baseline and target with the Supplier.	The SIAM Supplier shall work with the Other Suppliers to reduce the overall carbon footprint baseline of the Services in line with the agreed target and timeline.
Reporting		

Sustainability Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
e) every six months provide the SIAM and/or the Customer with a report aligned to support the production of the central government STAR (Sustainable Technology Annual Report) returns that the Customer must submit under its Greening Government Commitments and other reporting obligations and shall include as applicable; i) Server Rooms - measured by Total Power Consumptions KWhr and Carbon Data measured in Metric Tonnes (if known) • On-Premise server rooms/ Datacentre • Off-Premise Data Centre or Hosting facility • Public and Private Cloud • Other Servers i.e. Local Application Servers (LOAPS) • End User Devices - measured by Quantity (No.) • Desktop PC's, Laptops, Tablets, Smart Phones, Thin Clients, Other • Peripherals - measured by Quantity (No.) • Monitors/screens, Other ii) Networks (only include devices not included in hosting data) - measured by Quantity (No.) • 10/100 switches • 10/100/1000 switches • Core switches • Wireless access points • Room based hubs • Unmanaged edge switches • POE Class 1 • POE Class 2 • POE Class 3 • POE Class 4 • Other iii) Phones - measured by Quantity (No.)		

Sustainability Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
• PABX distributed, Locally powered VOIP phones, Mobile phones, Other i.e. POE iv) Imaging - measured by Quantity (No.) • Production mono MFD • Production colour MFD • MFD (colour) • MFD (b/w) • Laser printer • Inkjet • Scanner • Copier • Fax • Other imaging devices v) Audio Visual - measured by Quantity (No.) • Projectors, Screens, VC, Other AV equipment vi) Online Meetings - measured by total number initiated • Online meetings (i.e. Teams) vii) all ICT waste - measured by Quantity, Weight(kg) and Value Returned • categorised by: prevention, reuse, recycle, recovery and disposal;		
f) annually, provide a report detailing sustainability improvements, achievements, progress against targets, recommended energy saving technology and recommendations to reduce the environmental impact of the Services;		

2.20 Relationship Management Service

Relationship Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.20..1Outline The Supplier shall align its processes with the Relationship management Service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Relationship management service across the Customer's Services.		The SIAM Supplier design, provide and manage an effective relationship management process with each of the Other Suppliers, the Customer and other stakeholders, and through such relationships seek to ensure the delivery of best value for money, impeccable service experience to Users, and the realisation of the Service Levels.
2.20..2Scope All Relevant Services All the Other Suppliers The Customer and other stakeholders		
2.20..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.20..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
a) develop and maintain, good and effective relationships with each of the Other Suppliers, the Customer and other stakeholders, and through such relationships seek to ensure the	The Customer will advise the Supplier on	

Relationship Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
delivery of best value for money, impeccable service experience to Users, and the realisation of the Service Levels; b) engage with and input into up to 2, UK based User Groups per annum, each meeting typically no more than 2 hours long; c) engage with and input into up to 2, UK based Services promotion events per annum, each event typically no more than 3 hours long;	the Customer's priorities relating to matters arising for the User Groups.	

2.21 Quality Management Service

Quality Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.21..1Outline The Supplier shall align its processes with the Quality Management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Quality Management service across the Customer's Services. Schedule 11 (Collaboration Agreement) describes the general processes and ways of working with which the Suppliers shall comply whilst working together for the benefit of the Customer. This Paragraph describes how the parties will agree additional service-related standards and policies.		The SIAM Supplier shall design, provide and manage the Quality Management service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.21..2Scope All Relevant Services		
2.21..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.21..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Quality Plan		
a) provide reasonable co-operation, information, documentation, advice and assistance to the SIAM Supplier and/or the Customer to enable it to create a Quality Plan; b)		
Processes, standards, policies and inter-Supplier dependencies		

Quality Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
c) provide reasonable co-operation, information, documentation, advice and assistance to the SIAM Supplier and/or the Customer to allow them to build a comprehensive and consistent suite of ITIL aligned management processes, standards, policies and services for all aspects of the integration and delivery of the end to end Services; d) implement and maintain a comprehensive and internally consistent suite of the policies, processes and standards to be used to deliver the Relevant Services, each taking account of the people and technical considerations; and i) test and audit compliance with the agreed processes, procedures, standards and policies with the SIAM, identify the corrective and preventative actions required and ensure those actions are completed; e) agree the processes, standards and policies including all handovers and escalation procedures with the SIAM Supplier and/or the Customer; f) engage with and at least every six months, input into the Customer's Service Improvement Plan which identifies improvements that need to be made to the Supplier's management processes and standards;		The SIAM Supplier shall design and implement cross functional service management and other appropriate process interfaces to maintain a comprehensive and internally consistent suite of the processes and standards to be used to integrate and deliver the end to end Services, each taking account of the people and technical considerations.
Operation		
g) operate the Relevant Services in accordance with the agreed processes, standard and policies;		The SIAM Supplier shall agree the processes, standards and policies applicable to the Relevant Services with the Supplier.

2.22 User Satisfaction Management Service

User Satisfaction Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.22..1Outline The Supplier shall align its processes with the User satisfaction management Service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned User satisfaction management service across the Customer's Services.		The SIAM Supplier shall provide a comprehensive User satisfaction management service. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.22..2Scope All elements of the Relevant Services All elements of the Relevant Suppliers		
2.22..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.22..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
Service		
a) reflecting industry best practice, provide input to a process for measuring User satisfaction in relation to but not limited to: i) the overall Services; ii) individual transactions (e.g. incidents, requests, questions etc.); iii) new starter set up;		

User Satisfaction Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
b) as part of the measuring User satisfaction process, agree the format and content of a User satisfaction survey with the SIAM Supplier ensuring that User satisfaction can be measured, and as appropriate by different elements of the Services; c) provide input to and suggest appropriate survey questions for the User feedback survey as requested by the SIAM Supplier and/or Customer; d) implement any identified and agreed service improvements arising from the survey; e) implement changes, at no additional charge to the Customer where necessary to address a Supplier Default;	The Customer shall agree the number of Users who will be surveyed.	Each of the Other Suppliers shall provide input to and suggest appropriate survey questions for the User feedback survey as instructed by the Customer. The Central Service Desk Service Supplier shall, on a monthly basis, issue Customer User Feedback Surveys to a random sample of Users.

2.23 Performance Management Service

Performance Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.23..1Outline The Supplier shall align its processes with the Performance management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Performance management service across the Customer's Services.		The SIAM Supplier shall design, provide and manage the Performance management service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.23..2Scope All Relevant Services		
2.23..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.23..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
a) provide reasonable co-operation, information, documentation, advice and assistance to the SIAM Supplier to enable it to carry out its performance management function; b) work with the SIAM and/or the Customer to implement initiatives to improve Service Level achievement;		The SIAM Supplier shall keep any information disclosed to it by each of the Other Suppliers confidential, except where it has to disclose the information to perform its functions under this Schedule.

Performance Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
c) upon request, provide the SIAM Supplier and/or the Customer with access to the Suppliers monitoring systems so that the Customer can independently assess the Service Levels; d) provide the SIAM Supplier and/or the Customer with any reasonable information necessary for the Customer to review the Supplier's performance against the Service Levels; e) ensure performance failures are being captured, assessed and that preventative and corrective actions are, as appropriate, acted upon, to prevent repetition or reoccurrence; f) carry out any necessary corrective and service improvement activity;		

2.24 Escalation/Complaint Management Service

Escalation/Complaint Management service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.24..1Outline The Supplier shall align its processes with the Escalation/Complaint management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Escalation/Complaint management service across the Customer's Services.		The SIAM Supplier shall design and provide a comprehensive Escalation/Complaint management service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.24..2Scope All escalation, complaints or disputes related to the Supplier or the Relevant Services		The SIAM Supplier shall develop and agree an escalation procedure including a Call Escalation Procedure with the Customer and the Other Suppliers.
2.24..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays).		
2.24..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		Each of the Other Suppliers shall keep any information disclosed to it by each of the Other Suppliers confidential, except where it has to disclose the information to perform its functions under this Schedule

Escalation/Complaint Management service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
Process		
a) agree and comply with the process and procedures for accepting ownership of escalations/Complaints; b) co-operate with the SIAM Supplier and/or the Customer when they are managing and responding to User escalations whether escalated to Complaint status; and c) implement reasonable corrective action to address issues raised by the Complaint; d) liaise with SIAM Supplier, where the escalation/Complaint relates to an Other Supplier's Services; e) agree and comply with an escalation procedure, including for Call Escalation, with the SIAM and/or the Customer and the Other Suppliers; f) progress all escalations/Complaints to satisfactory resolution;	The Customer shall agree corrective action to be implemented by the Supplier to address issues raised by the escalation/Complaint.	The SIAM Supplier shall define and agree a User escalation/Complaints process and procedure with the Customer and the Other Suppliers for accepting ownership of Complaints. The Service Desk Supplier shall ensure the Central Service Desk Supplier has personnel/agents are trained in all aspects of the escalation/Complaint management process and agreed procedures.
Service Review Meetings		
g) at the monthly service review meetings or when requested by the SIAM Supplier and/or the Customer: i) propose and agree a plan to implement, reasonable corrective action to address issues raised by the escalation/Complaint;		

2.25 Onboarding Management Co-ordination Service

Onboarding Management Co-ordination Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.25..1Outline The Supplier shall align its processes with the comprehensive Onboarding Management co-ordination service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Onboarding Management co-ordination service to the Customer. **The charges for this service shall be determined as a Time and Materials payment mechanism using the Person Day Rates in Schedule 2 (Charges and Invoicing) at Part C (Supplier Personnel Rate Card). The initial effort cap shall be zero Person Days. This cap may be extended by the Customer in accordance with the Change Control Procedure.**		The SIAM Supplier shall provide a comprehensive exit strategy service in respect of the Other Suppliers to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.25..2Scope A new Other Supplier A new government department or organisation who is 'joining' the TrIS service		
2.25..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays)		
2.25..4Services To work with the Customer and the Other Suppliers, the Supplier shall:		
Onboarding		

a) agree with the Customer and the SIAM Supplier, an end to end plan describing the actions of each of the parties during the onboarding transition including those of the Other Suppliers, the new Other Supplier or the new government department/organisation; and i) shall input to and support the development of an induction guide for the new Other Supplier to describe how the Other Supplier collaborates in delivery of the Customer Services ii) review, and as appropriate, update the TrIS ITIL aligned management processes;		The SIAM Supplier shall produce and agree with the Customer and the Other Suppliers, an end to end plan describing the actions of each of the parties during transition including those of the Other Suppliers, the new Other Supplier or the new government department/organisation. The SIAM Supplier shall produce an induction guide for the new Other Supplier to describe how the Supplier and the Other Suppliers collaborate in delivery of the Customer Services. The SIAM Supplier shall review, and as appropriate, update the TrIS ITIL aligned management processes and communicating any changes to the Other Suppliers.

2.26 Exit Management Co-ordination Service

Exit Management Co-ordination service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.26..1Outline The Supplier shall align its processes with the comprehensive Exit Management co-ordination service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Exit Management co-ordination service to the Customer. **The charges for this service shall be determined as a Time and Materials payment mechanism using the Person Day Rates in Schedule 2 (Charges and Invoicing) at Part C (Supplier Personnel Rate Card). The initial effort cap shall be zero Person Days. This cap may be extended by the Customer in accordance with the Change Control Procedure.**		The SIAM Supplier shall provide a comprehensive exit strategy service in respect of the Other Suppliers to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.26..2Scope All the Other Suppliers		
2.26..3Service Hours 08:00-18:00 Monday to Friday (excluding UK Bank Holidays)		
2.26..4Services To work with the Customer and the Other Suppliers, the Supplier shall:		
Exit Strategies		
a) provide the Customer and the SIAM Supplier with any reasonable information necessary for the SIAM Supplier to provide this Service;		

b) agree the exit plan insofar as they are affected, and which describes the actions of each of the parties; c) comply with its obligations under the exit plan and assist the Customer to manage any associated transition to a Replacement Supplier	The Customer will work with the SIAM Supplier and with the Supplier where relevant, to agree an exit plan with the relevant Supplier concerned.	The SIAM Supplier shall keep any information disclosed to it by each of the Other Suppliers confidential, except where it has to disclose the information to perform its functions under its agreement with the Customer. .

2.27 Service Continuity Management Service

Service Continuity Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.27..1Outline The Supplier shall align its processes with the Service Continuity management service provided by the SIAM Supplier so as to create an end-to-end, seamless and ITIL aligned Service Continuity management service across the Customer's Services.		The SIAM Supplier shall in accordance with Schedule S6 (Business Continuity & Disaster Recovery), design and provide a comprehensive Service Continuity management service to the Customer. This includes, as necessary, directing the Other Suppliers on behalf of the Customer.
2.27..2Scope All the Relevant Services		
2.27..3Service Hours 08:00 - 18:00 Monday to Friday (excluding UK Bank Holidays)		
2.27..4Services To work with the SIAM Supplier, the Customer and the Other Suppliers, the Supplier shall:		
BCDR Plan		
a) develop and maintain a BCDR Plan in accordance with the requirements of Schedule S6 (Business Continuity and Disaster Recovery);	The Customer shall maintain its own BCDR	The SIAM Supplier shall monitor and regularly report to the

Service Continuity Management Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
b) in accordance with the requirements in this paragraph, ensure that a reviewed, updated, and up to date copy of the BCDR Plan is provided to the SIAM Supplier and/or the Customer at least every 12 months; c) provide reasonable support and assistance to the Customer to enable the Customer to ascertain their readiness, and capability to support the Customer to meet the Customer's BCDR (Business Continuity and Disaster Recovery) Plan and the Other Suppliers' individual BCDR plan.	Plan and will make this available to agreed Supplier representatives on request.	Customer on each of the Other Suppliers compliance with Schedule S6 (Business Continuity and Disaster Recovery). Each of the Other Suppliers shall develop and maintain a BCDR Plan in accordance with the requirements of Schedule S6 (Business Continuity and Disaster Recovery).

2.28 Procurement Service

Procurement Service		
Supplier Obligations	Customer Obligations	Other Supplier Obligations
2.28..1 Outline The Supplier shall provide a non-exclusive procurement service to the Customer.		
2.28..2 Scope All procurement of Relevant Goods and Relevant Services requested by the Customer.		
2.28..3 Service Hours 08:00 – 18:00 Monday to Friday (excluding UK Bank Holidays).		
2.28..4 Services To work with the Customer, the Supplier shall upon request:		
Operation		
a) provide the Customer with reasonable advice and guidance on the procurement of Goods or Services;		
b) provide the Customer with proactive and reasonable advice and guidance on how the Customer can reduce costs and maximise value with regard to its procurement;		
c) provide a procurement service to the Customer; and d) provide a single point of contact for all-procurement related activities;	The Customer shall have the right of rejection any quotation.	

Purpose

This Schedule sets out the following:

a) in Part One, provisions relating to Service Levels and Service Credits; and

b) in Part Two, other provisions relating to performance management.

Part One – Service Levels and Service Credits

Overview of Service Credit Points and Service Credits

This Part One sets out the mechanism by which Service Credits are calculated and valued.

Service Credits shall be payable by the Supplier in the event that the Supplier accrues Service Credit Points in any month.

Service Credits shall be applicable with effect from the first Actual Operational Service Commencement Date.

Service Credits are a reduction of the amounts payable in respect of the Services and do not include VAT. The Supplier shall apply the value of any Service Credits against the appropriate invoice in accordance with the provisions of Attachment 2 - Charges and Invoicing

The Supplier confirms that it has modelled the Service Credits and has taken them into account in setting the level of the Charges. Both Parties agree that the Service Credits are a reasonable method of price adjustment to reflect poor performance but may not reflect any damage, loss, cost or expense incurred by the Customer or any other party.

Service Credits are payable where any Service Level is not achieved (subject to the provisions of this Schedule). However, for all Service Levels, in the event of a failure by the Supplier to achieve a Service Level, the Parties shall discuss the failure and the reasons for it at the meeting of the Service Management Board in the month following the failure, and the Supplier shall take such steps as are necessary to ensure that the Service Level is achieved or exceeded in the future.

Classification of Service Levels

The table in Annex 1 (*Service Levels*) to this Schedule specifies:

a) the Service Levels;

b) the type of each Service Level; and

c) for Service Levels subject to Service Credits the amount of Service Credit Points which the Supplier will incur for failure to meet the relevant Service Levels.

Service Credits

Service Credit period
All Service Credits will be calculated monthly and payable in accordance with Paragraph 5.4 (Payment of Service Credits).

Calculation of Service Credits
Service Credits in respect of Service Levels shall be valued as a percentage of the related Service Charges for the month in which the Service Credit Points used to calculate the Service Credits accrue.

Part C (*Service Levels)* describes how the achieved levels of performance for each Service Level will be measured, and how Service Credit Points will be allocated for Performance Failures. If the Supplier fails to meet a Service Level or to monitor and report on a Service Level, it will accrue the number of Service Credit Points in accordance with the mechanisms specified in the table in Annex 1 (*Service Levels*) of this Schedule.

The number of points accrued by the Supplier during the relevant period will be totalled for all of the Service Levels to arrive at the number of points for the period.

The total number of points will be converted into a cash value. The cash value will be calculated on the basis that one Service Credit Point is worth 1% (one percent) of the Service Charges for the relevant month

Liability for Service Credits
The Supplier's liability for Service Credits is subject to Clause 32 (*Supplier Relief due to Buyer Cause*) *and Clause* 33 (*Force Majeure*).

Any dispute in terms of the level of any Service Credit or the Supplier's liability for the failure of the Service that leads to the Supplier incurring Service Credits will be resolved in accordance with Schedule 4 *(Dispute Resolution Procedure).*

Cap on Service Credits
The maximum value for all Service Credits accrued in respect of a month shall not under this Agreement exceed fifteen percent (15%) of the Service Charges for that month ("Service Credit Cap").

The liability of the Supplier in respect of Service Credits shall be subject to Clause 19 (*Limitation of Liability*) provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Credit Points in excess of such financial limit in accordance with the provisions of the Schedule.

Repeat Failures

If the Supplier fails to achieve any Service Level during 2 consecutive months the second such failure shall be a Repeat Failure.

Any subsequent failures by the Supplier to achieve that same Service Level in further consecutive months shall also be a Repeat Failure.

If any Repeat Failure occurs the number of Service Credit Points that shall accrue to the Supplier in respect of such Repeat Failure shall be the number of Service Credit Points that would normally accrue in respect of an initial failure of that Service Level (in accordance with the mechanisms set out in the table in Annex 1 (*Service Levels*) of this Schedule multiplied in accordance with the following table:

Number of Repeat Failures (whether or not in respect of the same Service Level)	Multiplier
0 (initial failure)	1
1 (first Repeat Failure)	1.5
2 (second Repeat Failure)	2
3 (third Repeat Failure)	3
Further Repeat Failures	3

Payment of Service Credits
Service Credits incurred during a monthly period will be offset against the Service Charges for that month or issued to the Customer as a credit note (at the Customer's option).

Measurement and Reporting of Service Credit Points and Service Credits

This Paragraph describes the manner in which the Service Levels, Service Credits and Service Credit Points will be measured and reported upon.

The Supplier shall be responsible for the calculation of Service Levels, Service Credit Points and Service Credits.

The Supplier shall monitor the performance of each of the Services by reference to the Service Level(s) for that Service and shall send the Customer a report each month within ten Working Days of the end of the preceding month with effect from the first Actual Operational Service Commencement Date detailing Service Level performance.

For any month, the Supplier's calculation of Service Levels, Service Credit Points and Service Credits shall be provided by the Supplier to the Customer's Service Manager for the purposes of the Service Management Board meeting in the month following the end of the applicable month.

The Customer's Service Manager shall either confirm his acceptance or rejection of the Supplier's calculation of the Service Levels, Service Credit Points and Service Credits within 10 Working Days of the meeting of the Service Management Board referred to in Paragraph 6.4 (*Measurement and Reporting of Service Credit Points and Service Credits*) above (any such acceptance or agreement being without prejudice to any subsequent identification of errors or other related faults and their associated liabilities and remedies).

Part Two – Other Performance Management Provisions

Principal points

This Part Two provides the methodology for monitoring the Services:

- to ensure that the Supplier is complying with the Service Levels; and
- for identifying any Incidents in the performance of the Supplier and/or delivery of the Services.

Development of the Performance Monitoring System

From the Effective Date the Supplier shall:

develop, consulting with the Customer, a performance monitoring system (the "**Performance Monitoring System**") that shall comply, without limitation, with relevant provisions of Attachment A - (*Services Specification*) and, as a minimum, cover how the following shall be addressed:

- notifications to the Central Service Desk of Incidents and other defects in the Supplier's performance and/or delivery of the Services;
- Supplier self monitoring, including using a suitable and appropriate service desk tool or mechanism;
- User satisfaction surveys (including the User Feedback Survey);
- performance reviews, covering processes, people and technology;
- support for Customer audits; and
- processes and systems to enable the Supplier to monitor effectively its performance of the Services against the Service Levels.

The description of the Performance Monitoring System shall additionally record:

- the format and content of the Performance Monitoring Report; and
- how the Supplier will comply with the obligations set out in this Part Two.

Within 20 Working Days of the Commencement Date the Supplier shall provide the Customer with the first draft description of its proposed Performance Monitoring System

Each Party shall use all reasonable endeavours to work together in reviewing and developing the draft Performance Monitoring System and to work towards agreement of a final draft definition of the Performance Management System. As part of working towards a final draft the Supplier shall produce re-drafted versions to reflect the Parties' discussions and any specific reasonable requests of the Customer.

The Parties agree that the development and implementation work for the Performance Management System shall be agreed and complete before the Planned Operational Services Commencement Date.

It is in the interests of the Parties to allow a short period of operational running (no more than 40 Working Days) after the first Actual Operational Service Commencement Date for refinement and

understanding the practical implications of the final draft and implemented Performance Monitoring System (without prejudice to the application of the Service Levels during that period).

Once the period of operational running is complete the documented Performance Monitoring System shall be agreed by the Parties and any implementation changes shall be applied and adopted immediately. If the Parties have not agreed the Performance Monitoring System within 40 Working Days of operational running the matter shall be resolved in accordance with the Dispute Resolution Procedure.

Maintenance and review of the Performance Monitoring System

The Performance Monitoring System (the description of which shall be a contract version controlled document managed as a Configuration Item) shall be maintained and updated on a monthly basis by the Supplier, as may be necessary to reflect the then current state of the Services. Details of any updated Performance Monitoring System shall be promptly forwarded to the Customer for approval. The Customer shall be entitled to require reasonable amendments to the updated Performance Monitoring System and the Supplier shall make such amendments and re-submit a further updated Performance Monitoring System to the Customer for approval. Until such time as the updated Performance Monitoring System is approved by the Customer the Performance Monitoring System then existing (this is to say prior to the update) shall continue to apply.

The Parties shall regularly consider and review the Performance Monitoring System at the Service Management Board meetings pursuant to Schedule 7 (*Governance*). The Customer shall be entitled to reasonably require, and the Supplier must comply with requests for, routine changes to the Performance Monitoring System.

Without prejudice to Paragraphs 9.1 and 9.2 (*Maintenance and review of the Performance Monitoring System*), each of the Customer and the Supplier shall have the right to propose any changes to the Performance Monitoring System (and agreement to such changes shall not be unreasonably withheld).

Performance monitoring and performance review

Within 5 Working Days of the end of each month, the Supplier shall provide a Monthly Service Management Report to the Customer's Contract Manager.

The Monthly Service Management Report shall be in the format set out in Annex 3 of Attachment 1 (*Services Specification*).

The draft Monthly Service Management Report shall be reviewed and its contents agreed by the Parties at the Service Management Board meeting which immediately follows the issue of such report in accordance with Paragraph 10.1 (*Performance monitoring and performance review*).

The Supplier shall provide the Customer with a Quarterly written summary of the monthly Performance Monitoring Reports that have been prepared during that quarter (Quarterly Service Management Report). The Quarterly Summary shall be provided by the Supplier to the Customer within 5 Working Days of the end of each Quarter, and shall be reviewed at the Service Management Board meeting which immediately follows its issue. The Quarterly Summary shall contain such additional details as the Customer shall reasonably require.

The aim is for all data provided as part of the Monthly Service Management Report and the Quarterly Service Management Report to be relevant to the Services Specification and the Customer's business needs. The reporting schedule and content will be reviewed regularly by the Parties to ensure this.

Feedback mechanisms will be built into all report formats to gauge relevance as part of this review process.

Satisfaction surveys

In addition to the surveys in relation to the User satisfaction, the Customer may undertake additional satisfaction surveys in respect of Registered Users or various groups of Registered Users. These surveys may consider:

the assessment of the Supplier's performance by the Registered Users; and/or

other suggestions for improvements to the Services.

The Customer shall be entitled to notify the Supplier of any aspects of the Services which the responses to the satisfaction surveys reasonably suggest are not meeting the required standard.

The Supplier shall, as soon as reasonably practicable after notification from the Customer in accordance with Paragraph 11 (*Satisfaction surveys*), ensure that such measures are taken by it as are appropriate to achieve such improvements as soon as is reasonably practicable.

Records

The Supplier shall keep appropriate documents and records in relation to the Services being delivered and the other requirements to be satisfied in accordance with Annex 3 (*Records Provision).*

The Supplier shall provide to the Customer such supporting documentation as the Customer may reasonably require in order to assess the level of the performance of the Services and the calculations of the amount of Service Credits for any specified period.

The Supplier shall ensure that the Performance Monitoring System and any variations or amendments thereto, the log of all Incidents held by the Central Service Desk , any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Customer are available to the Customer on-line and capable of being printed.

Call Escalation Procedure

Within 20 Working Days of the Effective Date the Supplier shall provide the Customer with the first draft description of its proposed Call Escalation Procedure to be followed in the event that an operational issue has arisen. The Call Escalation Procedure shall set out the criteria for escalation of operational issues (that may arise from calls reported to the Central Service Desk, or which may arise during the course of resolving an Incident or Problem, or which may arise for any other reason), and the escalation path to be followed within the Supplier's organisation.

The Call Escalation Procedure shall give the Customer the right to request:

- escalation of any Priority 1 call or Priority 2 call
- further escalation of any call that has been escalated to the Supplier's Service Manager.

The Call Escalation Procedure shall also contain provisions that, for all calls that are escalated at Customer request, the Supplier's Service Manager shall provide an analysis report demonstrating the actions taken to resolve the issue within the applicable Service Level.

Each Party shall use all reasonable endeavours to work together in reviewing and developing the draft Call Escalation Procedure and to work towards agreement of a final draft definition of the Call Escalation

Procedure. As part of working towards a final draft the Supplier shall produce re-drafted versions to reflect the Parties' discussions and any specific reasonable requests of the Customer.
The Parties agree that the majority of the development and implementation work for the Call Escalation Procedure shall be agreed and complete before the Planned Operational Services Commencement Date.

ANNEX 1 – Service Levels

Table 1 – Service Level Agreements
Table 2 – Key Performance Indicators

Table 1 Service Level Agreements

Ref	Service Area	Name	Description	SLA Target	Reporting Period	Service Credits
EUC SLA-1	Change Management	Change Implementation	Percentage of changes implemented successfully, in accordance with agreed deliverables, for which the supplier is responsible	Equal to or greater than 95%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1 Service Credit Points.
EUC SLA-2	Incident Management	Resolution of Incidents within SLA (P1)	Percentage of Priority Level 1 Incidents, assigned to End User Compute Supplier, resolved within 2 hours	Equal to or greater than 98%	Monthly	0.2 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-3	Incident Management	Resolution of Incidents within SLA (P2)	Percentage of Priority Level 2 Incidents, assigned to End User Compute Supplier, resolved within 4 hours	Equal to or greater than 98%	Monthly	0.2 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-4	Incident Management	Resolution of Incidents within SLA (P3)	Percentage of Priority Level 3 Incidents, assigned to End User Compute Supplier, resolved within 10 hours	Equal to or greater than 99%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-5	Incident Management	Resolution of Incidents within SLA (P4)	Percentage of Priority Level 4 Incidents, assigned to End User Compute Supplier, resolved within 20 hours	Equal to or greater than 99%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.

EUC SLA-6	Request Management	Resolution of Requests within SLA (P1)	Percentage of Priority Level 1 Requests, assigned to End User Compute Supplier, resolved within 1 hour	Equal to or greater than 98%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-7	Request Management	Resolution of Requests within SLA (P2)	Percentage of Priority Level 2 Requests, assigned to End User Compute Supplier, resolved within 8 hours	Equal to or greater than 98%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-8	Request Management	Resolution of Requests within SLA (P3)	Percentage of Priority Level 3 Requests, assigned to End User Compute Supplier, resolved within 20 hours	Equal to or greater than 99%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA-9	Request Management	Resolution of Requests within SLA (P4)	Percentage of Priority Level 4 Requests, assigned to End User Compute Supplier, resolved within 30 hours	Equal to or greater than 99%	Monthly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.
EUC SLA -10	Service Level Management	Customer Satisfaction (CSAT)	Percentage of Users who are satisfied or extremely satisfied with the quality of support they receive from the end user support engineers. Example Survey Responses (5 point scale): 1 = Extremely Dissatisfied 2 = Dissatisfied 3 = Neither Satisfied nor Dissatisfied 4 = Satisfied 5 = Extremely Satisfied	Equal to or greater than 85%	Monthly	0.2 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Points for this Service Level is 1 Service Credit Points.
EUC SLA-11	Incident Management	Mean Time to Resolve	Percentage decrease in the elapsed time from when an Incident is raised to when an Incident is resolved.	Equal to or greater than 5% improvement on total call resolution time, Quarter on Quarter	Quarterly	0.1 Service Credit Point per each percentage that deviates from the target. The maximum Service Credit Point for this Service Level is 1.5 Service Credit Points.

Table 2 – Key Performance Indicators

Ref	Service Area	Name	Description	KPI Target	Reporting Period
EUC KPI-1	Release and Deployment Management	Release Implementation	Percentage of releases which are deployed that are successful and in the committed timeframe.	Equal to or greater than 98%	Monthly
EUC KPI-2	Service Asset and Configuration Management	Number of CMDB errors	Number of errors found in the CMDB as a result of an audit.	Equal to or less than 5%	Quarterly
EUC KPI-3	Continual Service Improvement	Automation of EUC activities	Percentage increase in the use of automation and self-service in respect to EUC activities to support a shift left culture	Equal to or greater than 5%	Quarterly
EUC KPI-4	Service Management Oversight	Response time to Parliamentary Questions (or other Ministerial queries) and requests received under the FOIA	Response time to PQs/Ministerial queries shall be 4 Working Hours. Response time to FOIA requests shall be 2 Working Days. The response time period will begin at the time of receipt of the request from the Customer.	Equal to 100%	Monthly
EUC KPI-5	Incident Management	Mean Time Between Failures	Percentage increase in the elapsed time between inherent failures of an End User Device or Peripheral, during normal operation.	Equal to or greater than 5% improvement on failure rate, Quarter on Quarter.	Quarterly
EUC KPI-6	Incident Management	Reduction in the number of SLA breaches	Percentage reduction in the number of breached Incidents during reporting period	Equal to or greater than 5% improvement on breach rate, Quarter on Quarter.	Quarterly
EUC KPI-7	Request Management	Reduction in the number of SLA breaches	Percentage reduction in the number of breached Request during reporting period	Equal to or greater than 5% improvement on breach rate, Quarter on Quarter.	Quarterly

EUC KPI-8	Service Level Management	Customer Complaints	Number of received customer complaints during reporting period	Equal to or less than 0.1% of all closed Incidents and request during period for which the End User Computing Supplier is responsible	Quarterly

Crown Commercial Service

ANNEX 2 - Outline Performance Monitoring System

The Performance Monitoring System will encompass processes that allow a reporting structure to ensure that the performance of all Services, including the Service Desk, is transparent to the Customer. Outputs will show, across all Services, trend analysis and, where possible, projected future performance. Reports will be delivered in accordance with the timeframe specified in Paragraph 10 (*Performance monitoring and performance review*)) and Attachment 1 (*Services Specifications*) to allow analysis prior to relevant meetings. The reports shall include those listed at Annex 3 *(Reports)* to the Services Specification.

All Supplier reporting should be available via an online (real-time or the latest version) dashboard or report as the default delivery method unless where otherwise agreed with the Customer.

Crown Commercial Service

ANNEX 3 – Records Provision

Reports

The Customer may require any or all of the following reports:

- delay reports;
- reports relating to Testing and Tests carried out under Schedule S3 (Security Requirements (Part Two)) and Schedule S6 (Business Continuity and Disaster Recovery);
- reports which the Supplier is required to supply as part of Attachment 1 (Services Specification);
- annual reports on the Insurances;
- security reports; and
- Force Majeure Event reports.

Records

The Supplier shall retain and maintain all the records (including superseded records) referred to in Services Specification Part C, Annex 4 (*Records to be kept by the Supplier*) in accordance with Paragraph 29 of the Call Off Terms *(Records and Audit)*

Crown Commercial Service

ANNEX 4: Records to be kept by the Supplier

The records to be kept by the Supplier are:

1 this Agreement, its Schedules and all amendments to such documents;
2 all other documents which this Agreement expressly requires to be prepared;
3 records relating to the appointment and succession of the Supplier Representative and each member of the Key Personnel;
4 notices, reports and other documentation submitted by any Expert;
5 all operation and maintenance manuals prepared by the Supplier for the purpose of maintaining the provision of the Services and the underlying IT Environment and Supplier Equipment;
6 documents prepared by the Supplier or received by the Supplier from a third party relating to a Force Majeure Event;
7 all formal notices, reports or submissions made by the Supplier to the Customer Representative in connection with the provision of the Services;
8 all certificates, licences, registrations or warranties in each case obtained by the Supplier in relation to the provision of the Services;
9 documents prepared by the Supplier in support of claims for the Charges;
10 documents submitted by the Supplier pursuant to the Change Control Procedure;
11 documents submitted by the Supplier pursuant to invocation by it or the Customer of the Dispute Resolution Procedure;
12 documents evidencing any change in ownership or any interest in any or all of the shares in the Supplier and/or the Guarantor;
13 invoices and records related to VAT sought to be recovered by the Supplier;
14 financial records, including audited and unaudited accounts of the Guarantor and the Supplier;
15 records required to be retained by the Supplier by Law, including in relation to health and safety matters, health and safety files and all consents;
16 all documents relating to the insurances to be maintained under this Agreement and any claims made in respect of them;
17 all other records, notices or certificates required to be produced and/or maintained by the Supplier pursuant to this Agreement; and
18 all audit trail data referred to in Schedule S3 (*Security Requirements)*.

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	*[insert description]*	*[insert amount]*	*[insert date as per Outline Implementation Plan]*	*[insert amount]*
M2				
M3				
M4				
M5				

Part B – Service Charges

Charge Number	Service Charges
[Service Line 1]	
[e.g. SL1C1]	
[Service Line 2]	
[e.g. SL2C1]	

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

Staff Grade	Day Rate (£)

Part D – Risk Register

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 12
Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Owner

Part E – Early Termination Fee(s)

To be confirmed

Crown Commercial Service

Attachment 3 – Outline Implementation Plan

To be confirmed

#	Milestone	Deliverables (*bulleted list showing all Deliverables (and associated tasks) required for each Milestone*)	Duration (*Working Days*)	Milestone Date
M1	[Concept Design]	[Statement of Requirements System/Application Specifications Interface Specifications Systems Testing Strategy Implementation Strategy and Plan Risk and Issues Management Plan Outline Disaster Recovery Plan Project Schedule Service Management Plan]		
M2	[Full Development]	[Design Verification Reports Design Validation Reports Change Management Plan System/Application Implementation Plan Risk and Issues Management Project Schedule Service Management Plan]		
M3	[System User Testing]	[System Test Report Risk and Issues Management Plan Project Schedule Service Management Plan Defects Log Final Inspection and Testing Report]		
M4	[User Readiness for Service]	[Training Plan Risk and Issues Log Implementation Plan Operations Plan Data Conversion & Cutover Plan Project Schedule Service Management Plan]		
M5	[Implementation]	[Implementation Plan Training Scripts]		
M6	[In Service Support]	[Post Implementation Report Data Conversion and Cut-Over Plan Service Delivery Reports Risk and Issues Log Service Management Plan Defects Log]		

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

To be confirmed

Service Levels and Service Credits

Service Levels				**Service Credit for each Service Period**
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
[Accurate and timely billing of Buyer]	[Accuracy /Timelines]	[at least 98% at all times]	[ ]	[0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure]
[Access to Buyer support]	[Availability]	[at least 98% at all times]	[ ]	[0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure]

The Service Credits shall be calculated on the basis of the following formula:

[Example:

Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance)	=	x% of the Service Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer
Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)	=	23% of the Service Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer]

Service Credit Cap

[Insert details of the Service Credit Cap]

Crown Commercial Service

Critical Service Level Failure

[Insert details of the Critical Service Level Failure – examples are provide below for guidance.]

[In relation to [specify the relevant Service Level] a Critical Service Level Failure shall include a delay in producing [specify the relevant Deliverable] ordered by the Customer in excess of [specify the relevant time period] more than once in any [specify the relevant period] or more than [specify the relevant time period].

And/or

In relation to [specify the relevant Service Level] a Critical Service Level Failure shall include a loss of [specify the relevant Availability] during core hours [specify the relevant core hours] to the [specify the relevant Service] for more than [specify the relevant time period], or [specify the relevant time period].]

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

.44.1 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
Tamsin Fendley	To be confirmed	[To be confirmed - Contract Period or insert alternative timescale]
Mike Thomas	Bid Management	[To be confirmed - Contract Period or insert alternative timescale]
To be confirmed		[To be confirmed - Contract Period or insert alternative timescale]

Part B – Key Sub-Contractors

Not applicable

Crown Commercial Service

Attachment 6 – Software

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

.44.2 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
To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed

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
To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed	To be confirmed

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

PART A – CREDIT RATING THRESHOLD

Entity	**Credit Rating (long term)** *(insert credit rating issued for the entity at the Commencement Date)*	**Credit Rating Threshold** *(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3)*
Supplier	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]
[Guarantor]	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]

PART B – RATING AGENCIES

- [Rating Agency 1 (e.g Standard and Poors)]
  - Credit Rating Level 1 = [AAA]
  - Credit Rating Level 2 = [AA+]
  - Credit Rating Level 3 = [AA]
  - Credit Rating Level 4 = [AA-]
  - Credit Rating Level 5 = [A+]
  - Credit Rating Level 6 = [A]
  - Credit Rating Level 7 = [A-]
  - Credit Rating Level 8 = [BBB+]
  - Credit Rating Level 9 = [BBB]
  - Credit Rating Level 10 = [BBB-]

- Etc.

- [Rating Agency 2 (e.g Moodys)]
  - Credit Rating Level 1 = [Aaa]
  - Credit Rating Level 2 = [Aa1]
  - Credit Rating Level 3 = [Aa2]
  - Credit Rating Level 4 = [Aa3]
  - Credit Rating Level 5 = [A1]
  - Credit Rating Level 6 = [A2]
  - Credit Rating Level 7 = [A3]
  - Credit Rating Level 8 = [Baa1]
  - Credit Rating Level 9 = [Baa2]
  - Credit Rating Level 10 = [Baa3]
  - Etc.

- [Rating Agency 3 (etc.)]
  - Credit Rating Level 1 = [XXX]
  - Etc.

- Attachment 8 – Governance

PART B – LONG FORM GOVERNANCE

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

SERVICE MANAGEMENT BOARD	
Buyer Members of Service Management Board (include details of chairperson)	To be confirmed
Supplier Members of Service Management Board	To be confirmed
Start Date for Service Management Board meetings	To be confirmed
Frequency of Service Management Board meetings	To be confirmed
Location of Service Management Board meetings	To be confirmed

Programme Board	
Buyer members of Programme Board (include details of chairperson)	To be confirmed
Supplier members of Programme Board	To be confirmed
Start date for Programme Board meetings	To be confirmed
Frequency of Programme Board meetings	To be confirmed
Location of Programme Board meetings	To be confirmed

Change Management Board	
Buyer Members of Change Management Board (include details of chairperson)	To be confirmed
Supplier Members of Change Management Board	To be confirmed
Start Date for Change Management Board meetings	To be confirmed
Frequency of Change Management Board meetings	To be confirmed
Location of Change Management Board meetings	To be confirmed

Technical Board	
Buyer Members of Technical Board (include details of chairperson)	To be confirmed
Supplier Members of Technical Board	To be confirmed
Start Date for Technical Board meetings	To be confirmed
Frequency of Technical Board meetings	To be confirmed
Location of Technical Board meetings	To be confirmed

Risk Management Board	
Buyer Members for Risk Management Board (include details of chairperson)	To be confirmed
Supplier Members for Risk Management Board	To be confirmed
Start Date for Risk Management Board meetings	To be confirmed
Frequency of Risk Management Board meetings	To be confirmed
Location of Risk Management Board meetings	To be confirmed

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

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: **Peter Beglin** privacy@hmtreasury.gov.uk

1.1.1.1 The contact details of the Supplier's Data Protection Officer are: Mike Thomas DPO@centerprise.co.uk

1.1.1.2 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.3 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: Full name Workplace address Workplace Phone Number Workplace email address Job Title or Role Range/Grade of role Date of start or return Home address (where required for delivery of remote working equipment only) Date of end of fixed term appointment, loan, placement or secondment Organisation Team Team's assigned desk location Line Manager's Name Line Manager's email address Line Manager's phone number Type of joiner Telephone pick up or hunt group Email distribution list membership Mailbox access Photographic Facial Image **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. *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	For the duration of the Framework Contract plus 7 years.
Nature and purposes of the processing	For the exchange of information between the Parties to this contract.
Type of Personal Data	Full name Workplace address Workplace Phone Number Workplace email address Job Title or Role Range/Grade of role Date of start or return Home address (where required for delivery of remote working equipment only) Date of end of fixed term appointment, loan, placement or secondment Organisation Team Team's assigned desk location Line Manager's Name Line Manager's email address Line Manager's phone number Type of joiner Telephone pick up or hunt group Email distribution list membership Mailbox access Photographic Facial Image
Categories of Data Subject	Contractors, Service Providers, Suppliers
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	For the duration of the Framework Contract plus 7 years.

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
[Performance]	To be confirmed		
[Charges]			
[Key Sub-Contractors]			
[Technical]			
[Performance management]			

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

Supplier's Proposal

REDACTED TEXT under FOIA Section 43 Commercial Interests.