Crown Commercial Service

Managed Infrastructure Services (MIS)- Datacentres Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated [redacted] 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 [redacted] 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 – Supplier Solution and 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).

Crown Commercial Service

Section A
General information

Contract Details	
Contract Reference:	C295183
Contract Title:	MANAGED INFRASTRCUTURE SERVICES (MIS)- DATACENTRES
Contract Description:	Management and operation of existing services hosted at the Crown Hosting Datacentres without any business disruptions while supporting the increased use of Cloud Computing services in line with the Authority DDaT strategy.
Contract Anticipated Potential Value:	£5.7M Ex VAT
Estimated Year 1 Charges:	[redacted]
Commencement Date:	22 AUGUST 2024

Buyer details

Buyer organisation name
NHS BUSINESS SERVICES AUTHORITY

Billing address
Stella House, Goldcrest Way, Newburn Riverside Park, Newcastle upon Tyne, NE15 8NY

Buyer representative name
[redacted]

Buyer representative contact details
[redacted]

Buyer Project Reference
C202593

Supplier details

Supplier name

Crown Commercial Service

AGILISYS LIMITED

Supplier address
Scale Space, Imperial College White City Campus, 58 Wood Lane, London W12 7RZ

Supplier representative name
[redacted]

Supplier representative contact details
[redacted]

Order reference number or the Supplier's Catalogue Service Offer Reference Number
Not Applicable

Guarantor details

Guarantor Company Name
The guarantor organisation name

NOT APPLICABLE

Guarantor Company Number
Guarantor's registered company number

NOT APPLICABLE

Guarantor Registered Address
Guarantor's registered address

NOT APPLICABLE

Crown Commercial Service

Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed	
1. TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2. TRANSITION & TRANSFORMATION	☐
3. OPERATIONAL SERVICES	
a: End User Services	☐
b: Operational Management	**X**
c: Technical Management	☐
d: Application and Data Management	☐
5. SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
22 AUGUST 2024

Contract Period

Initial Term	**Extension Period (Optional)**
2 YEARS	2 X 1-YEAR

Minimum Notice Period for exercise of Termination Without Cause
NOT APPLICABLE

Sites for the provision of the Services

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

Stella House, Goldcrest Way, Newburn Riverside Park, Newcastle upon Tyne, NE15 8NY

Supplier Premises:

Scale Space, Imperial College White City Campus, 58 Wood Lane, London W12 7RZ.

Third Party Premises:

Crown Commercial Service

Not Applicable

Buyer Assets
See C202593 Managed Infrastructure Services (MIS)- Datacentres Statement of Requirements

Additional Standards

Not Applicable

Buyer Security Policy

See NHSBSA Information Security Policy

Buyer ICT Policy

Not Applicable

Insurance

Third Party Public Liability Insurance (£) - £10,000,000

Professional Indemnity Insurance (£) - £10,000,000

Buyer Responsibilities

1. Provide unescorted access to crown hosting data centres 24x7.
2. Provide the ability to discuss our utilisation with Crown Hosting, so that we can report against power utilisation and data centre carbon footprint.
3. Provide a separate dedicated subscription within the Authority's existing Azure tenancy, for the Supplier to deploy and manage Arc management, Sentinel integration, Microsoft Defender and optionally Azure Backup for Crown Hosted services.
4. Arrange for Crown Hosting Data Centres to provide Scope 2 emissions data to the Supplier.
5. Such other Buyer Responsibilities as expressly set out elsewhere in the Agreement.

Goods

Not Applicable

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**

Crown Commercial Service

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 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 £500; and
- for the purpose of Paragraph 8.2.2, the figure shall be £10,000.

Crown Commercial Service

Section C

Part A - Additional and Alternative Buyer Terms

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

Part A – Additional Schedules

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

Part B – Additional Clauses

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

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

Part C - Alternative Clauses

Not used.

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

Additional Schedule S3 (Security Requirements)

A security management plan shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

90 Working Days

Additional Schedule S4 (Staff Transfer)

Crown Commercial Service

Not Applicable

Additional Clause C1 (Relevant Convictions)

Not Applicable

Additional Clause C3 (Collaboration Agreement)

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

90 Working Days

Section D
Supplier Response

Commercially Sensitive information

Not Applicable

Crown Commercial Service

Section E
Contract Award

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

SIGNATURES

For and on behalf of the Supplier

For and on behalf of the Buyer

Crown Commercial Service

Attachment 1 – Services Specification

Section 1 Introduction

This Statement of Requirements sets out the intended scope of the services to be provided by the Supplier and provides a description of what each service entails.

The Authority has two key outcomes it requires from this agreement. These are, first, a new supplier to take on the management and operation of our existing Infrastructure services hosted in Crown Hosting Data Centre (CHDC) facilities from the incumbent supplier without any business disruptions. Secondly demonstrable progress in supporting the Authority Digital, Data and Technology (DDAT) strategy, particularly in respect of the increased use of cloud computing Services and a reciprocal reduction in the usage of CHDC facilities, **as may be required during the life of the contract.**

The structure of the document is as follows.

1.1. Operational Services

1.1.1. Hosting Services being in (summary) management of existing Infrastructure services, including all Hardware and Software (up to and including operating systems) that is currently in place to support day to day operation of our key business services. Appendix 1 describes the current operational environment.

1.1.2. Technical Services Backup, Restore & Archive Services, being in (summary) ongoing management of the organisations data in line with our Backup Strategy and data retention policies.

1.1.3. Increase use of Cloud Computing, being in (summary) supporting the organisations DDAT strategy in providing a range of innovation and migration activities to increase the use of cloud computing while reducing the organisations footprint in CHDC. This requirement shall be delivered as an optional service.

1.1.4. Service Management Services, being in (summary) service to perform the Authority's service management processes and procedures for the Operational Services.

1.1.5. Security Management, being in (summary) the supplier must comply with the organisation's Information Security policies, standards, and procedures, in ensuring we continue comply with our compliance requirements (PSN, NHS DSPT). The expectation is that supplier will comply with guidance and standards issued by the National Cyber Security Centre (NCSC).

1.1.6. Interface Requirements, being in (summary), the Supplier shall ensure that the integration between the Supplier Applications and Authority Applications (including between the Supplier's monitoring and management suite(s) is preserved during and after any new Releases or upgrades.

1.1.7. The Collaboration Agreement and the ITSM policies, processes and procedure documents set out the management obligations/responsibilities.

1.1.8. Other Authority Requirements

Crown Commercial Service

1.2. Definitions

In this Statement of Requirements, the following expressions shall have the following meanings:

Defined term	Meaning
"Access Management"	is as defined under ITIL.
"Authority Applications"	Those applications used within the NHSBSA including COTS (Commercial Off-the-Shelf Software) and Data, and which list shall be updated from time to time by the Authority and notified to the Supplier
"Authority ITSM Reports"	Reports produced by the ITSM based on Supplier Data and Authority Data about the Technical Services and Hosting Services
"Authority **ITSM** Reports"	Reports produced by the **ITSM** based on Supplier Data and Authority Data about the performance of the Technical Services and Hosting Services.
"Authority's Services"	Services provided by the Supplier, services provided by the other Suppliers, and services provided by the Authority.
"Authority's ServiceDesk"	The Authority's service desk, which includes the "Service Desk" function defined under ITIL; it is the single point of contact for End Users and provides an interface for service operation processes and activities; is primary aim is to restore normal service (Incidents) as quickly as possible; it may be provided by the Authority or outsourced by the Authority.
"Availability"	Is as defined under ITIL.
"Bill of Materials"	A list of items required to be procured by the Supplier to enable the Supplier to deliver the Services.
"Capacity Management"	Is as defined under ITIL.
"Capacity"	Is as defined under ITIL.
"Change"	Is as defined under ITIL, and any other definitions of the same term elsewhere in the **Call Off Contract** shall not apply in this Statement of Requirements.
"Change Management"	Is as defined under ITIL.
"Change Management Process"	the Authority Change Management process ('Change Management' being as defined under ITIL).
"Cloud"	Cloud computing, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal manage effort or service provider interaction as further defined by NIST (the National Institute of Standards and Technology, US Department of Commerce) NIST SP 800-145, The NIST Definition of Cloud Computing
"Configuration"	Is as defined under ITIL.
"Configuration Items" or "CIs"	Is as defined under ITIL.
"Configuration Management"	Is as defined under ITIL.

"Configuration Management System"	Is as defined under ITIL.
"Continual Service Improvement"	Is as defined under ITIL.
"Continual Service Improvement Programme"	the Authority's programme for Continual Service Improvement
"Data"	data, whether stored in a structured or unstructured format.
"Data Centres"	any data centre colocation services used by an Incumbent Supplier, Crown hosting services (CHS).
"Database Services"	Distributed and centralised data base services.
"Definitive Media Library" or "DML"	Is as defined under ITIL.
"Demand Management"	Is as defined under ITIL.
"Deployment"	Is as defined under ITIL.
"Design Authority"	a design authority board within the Authority to provide assurance and ensure adherence to the Authority Digital, Data and Technology (DDaT) Strategy.
"Early Life Support (ELS)"	Is as defined under ITIL.
"Event"	Is as defined under ITIL.
"Event Management"	Is as defined under ITIL.
"High Availability Services"	Those Hosting Services and Technical Services which must be available across multiple locations and/or multiple Platforms in the same location.
"Hosting Services"	are described in paragraph 3.2(b) of this Statement of Requirements.
"Incident Resolution"	Is as defined under ITIL.
"Incident"	Is as defined under ITIL.
"Incumbent Supplier"	an incumbent supplier to the Authority for services similar to the Operational Services prior to the Effective Date.
"ITIL"	the most current version of the ITIL as published by Axelos Limited, a company incorporated and registered in England and Wales with company number 08489114 whose registered office is at 17 Rochester Row, London, SW1P 1QT as may be amended from time to time; as at November 2023, the glossary containing ITIL definitions is available (subject to

	acceptance of terms) via https://www.axelos.com/resource-hub/glossary/
"ITSM Tool"	the Authority's provided workflow management system for handling Incidents, Service Requests, Problems and Changes and other ITIL -aligned processes; it provides a central repository for all Data relating to the Authority's Services.
"ITSM"	IT Service Management, as defined by ITIL: The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology. An Authority-provided function accountable for the end-to-end delivery of services and the business value the Authority receives in relation to the Authority's Services; the function is accountable for end-to-end service governance (including standards and performance monitoring), management, integration, assurance and co-ordination. Performed by an IT service provider through an appropriate mixed people, process, and information technology.
"Knowledge Articles"	any recorded information, data, code, or other form of knowledge.
"Known Errors"	Is as defined under ITIL.
"Major Incident"	Is as defined under ITIL.
"Management Information"	Is as defined under ITIL.
"Master Time Reference"	a precision clock that provides timing signals to synchronise slave clocks using the standard Network Time Protocol; the clock is supplied by the Other Supplier that provides network infrastructure services.
"NCSC"	the National Cyber Security Centre, or its successor.
"Platforms"	the hardware platforms and core software for hosting the Authority Applications and operating the Technical Services.
"Preferred Target Date"	or such other date as is agreed in writing between the Authority and the Supplier.
"Problem"	Is as defined under ITIL.
"Problem Management"	Is as defined under ITIL.
"Recovery Point Objective" or "RPO"	Is as defined under ITIL.
"Recovery Time Objective" or "RTO"	Is as defined under ITIL.
"Release"	Is as defined under ITIL.
"Request Fulfilment"	Is as defined under ITIL.
"Service Acceptance Criteria"	Is as defined under ITIL.
"Service Acceptance"	Is as defined under ITIL as "Acceptance".
"Service Asset"	Is as defined under ITIL.
"Service Catalogue"	Is as defined under ITIL.
"Service Design Package"	Is as defined under ITIL.
"Service Level Management"	Is as defined under ITIL.
"Service Management Services Requirements"	the Authority's requirements for the Service Management Services set out in **Annex 2** to this Statement of Requirements.
"Service Owner"	Is as defined under ITIL.
"Service Requests"	Is as defined under ITIL.

"SKMS"	Stands for Service Knowledge Management System and is as defined under ITIL.
"Standard Change"	Is as defined under ITIL.
"Supplier Applications"	any Software applications provided by the Supplier (for its own use the use of the Authority or the use of the Other Suppliers) to other the Services.
"Supplier Approved Personnel"	those Supplier Personnel responsible for delivering the Services to the Authority or the Other Suppliers and/or those Supplier Personnel that are responsible for requesting and/or approving Changes or other matters relevant to the performance of the **Call Off Contract**.
"Supplier Data"	data provided by the Supplier in relation to the Services.
"Supplier User Access Control Policy"	a policy defining which systems, individuals or groups of users will be granted access to information or resources.
"Target Operating Model"	the future DDAT target operating model for DDAT provision across the Authority's functions and services which is a disaggregated supplier service and commercial model with a mix of insourced and outsourced functions.
"Technical Dependency Register"	a register of services (including the Services) on which the Authority, the Supplier and/or the Other Suppliers are dependent to provide their services; in the case of the Services, the initial version of that element of the register is as set out in Schedule 3 (Authority Responsibilities).
"Technical Services"	Are described in paragraph 2.3(c) of this Statement of Requirements.
"Transition Planning and Support"	Is as defined under ITIL.
"Workarounds"	Is as defined under ITIL.

Crown Commercial Service

Section 2 Service Descriptions

2.1. Operational Services

2.1.1. The Operational Services consist of Hosting Services, Technical Services, and Service Management Services.

2.1.2. These Operational Services will enable the Authority to operate its DDAT function and services under the Target Operating Model

2.1.3. Operational Hours are Monday to Friday 07:00 to 18:00 (excluding bank and public holidays in England, UK (United Kingdom) Local Time.

2.1.4. The Supplier shall provide an up-to-date contact to work with our major incident management (MIM) team to support any P1 related incidents that occur within the CHDC outside our normal business hours.

2.1.5. Operational Service Commencement Date for all Operational Services listed in this paragraph 3.1 will be no later than the Preferred Target Date

2.1.6. Operational Services must have a single Service Owner within the Supplier who is responsible for the overall management and development of the Operational Services

2.1.7. The Supplier shall supply Authority Data to the Authority in an industry standard format as requested by the Authority.

2.1.8. Unless otherwise directed by the Authority, the Supplier is required to safely dispose of all Supplier Equipment at the end of life of that Supplier Equipment.

2.2. Hosting Services

2.2.1. Hosting Services will consist of services hosted in CHDC. These services must combine to provide an efficient solution. The Hosting Services shall provide capabilities that enable the Authority, the Supplier, and the Other Suppliers to deliver the Authority's requirements.

2.2.2. CHDC The Authority has commissioned data centre colocation services from Crown Hosting Data Centres Ltd for the use of the Supplier to host and manage any infrastructure required to host the Authority Applications and operate the Technical Services.

2.2.3. The Hosting Services must continue to provide the following.

2.2.3.1. Environments

2.2.3.1.1. **Live environments.** The provision, management, and Availability of Platforms. Live environments include High Availability Services and disaster recovery.

2.2.3.1.2. **Non live environments** such as development, testing, and training are provisioned, managed and available for Authority Applications' Releases.

2.2.3.2. Distributed Platform Services (services distributed across more than one geographic location)

2.2.3.2.1. **Distributed server builds.** The creation, management, and maintenance of Deployment packages for operating system and supporting system software to distributed hosted server hardware or virtual machines, based on a standard Configuration including security hardening such that all relevant patches are implemented in a timely and controlled manner to maintain operational integrity.

2.2.3.2.2. **Distributed virtualisation and shared Platforms.** The design, build, testing and management of the Supplier-provisioned compute (server) and storage environments and management software to support virtual or shared distributed compute (server) environments and make the best use of Cloud and/or on-premises infrastructure to achieve optimum efficiency and agility and avoid over provision of Capacity.

2.2.3.2.3. **Distributed web hosting Platform services.** The creation and Deployment of packages for preconfigured distributed environments, which allow the hosting and delivery of web applications and services.

2.2.3.2.4. **Distributed High Availability Services**. The design, build, test, and management of High Availability Services, including DNS, DHCP, load balancing, database Platforms, web hosting Platforms and midrange services Platforms.

2.2.3.2.5. **Distributed database Services.** The design, build, test and Deployment of database Platform, and operational and technical maintenance and upgrades.

2.2.3.3. Centralised Platform Services (hosted in a single geographic location):

2.2.3.3.1. **Centralised server builds.** The creation, management, and maintenance of Deployment packages for operating system and supporting system software to centralised hosted server hardware or virtual machines, based on a standard Configuration including security hardening such that all relevant patches are implemented in a timely and controlled manner to maintain operational integrity.

2.2.3.3.2. **Centralised virtualisation and shared Platforms.** The design, build, testing and management of the Supplier-provisioned compute (server) and storage environments and management software to support virtual or shared centralised compute (server)environments and make the best use of Cloud and/or on-premises infrastructure to achieve optimum efficiency and agility and avoid over provision of Capacity.

2.2.3.3.3. **Centralised web hosting Platform services.** The creation and Deployment of packages for preconfigured centrally hosted environments, which allow for the hosting and delivery of web applications and services.

2.2.3.3.4. **Centralised High Availability Services.** The design, build, test, and management of High Availability Services, including DNS, DHCP, load balancing, database Platforms, web hosting Platforms and midrange services Platforms.

2.2.3.3.5. **Centralised database services.** The design, build, test and Deployment of database Platform, and operational and technical maintenance and upgrades.

2.2.3.4. Storage:

2.2.3.4.1. **Unstructured data services.** The design, build, allocation, and the management of the storage of raw data in such a way that will allow it to be consumed by Authority Applications, related services, and End Users, including data in the file store.

2.2.3.4.2. **Structured data services.** The design, build, allocation, and the management of storage of data normally associated with, but not limited to, applications, databases and also associated metadata. These services must make the best use of storage and avoid over provision and/or over allocation of storage with the ability to vary allocation to meet peak and normal patterns of demand in an agile manner.

2.2.3.5. Core Network and LAN Services (within CHDC):

2.2.3.5.1. **LAN Services.** The provision, Configuration, management and Availability of the Core and LAN network devices and software, to support the storage and server network. Collaborative working with the Other Suppliers is a requirement.

2.2.3.5.2. **Firewall Services**. The provision, Configuration, management and Availability of the firewall devices and core software, to secure and support the storage and server network. Collaborative working with the Other Suppliers is a requirement.

2.3. Technical Services

2.3.1. Backup and Recovery Services:

2.3.1.1. The provision of a backup service, including infrastructure, this will potentially include backups from the Local Server Rooms on BSA premises. The design and implementation of backup schedules, with timings which will not adversely impact on the Authority's service delivery, to ensure the operational data is regularly backed up to meet the Authority's Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The RTO is initially set out in the Authority's Information Governance policy and procedures and shall be contained in the Supplier's BCDR Plan. The RPO is set out in **Annex 3.**

2.3.1.2. The provision of a recovery service, to provide restoration of data from backups to the operational environment including self-service data retrieval. The design and implementation of recovery processes.

2.3.1.3. The service needs to meet the principles for protecting the organisation from Ransomware attacks as outlined in the National Cyber Security Centre guidance Principles for ransomware-resistant cloud backups - NCSC.GOV.UK

2.3.1.4. The backup solution must comply with, and the supplier should evidence their compliance with the latest version of NCSC's Offline Backup Guidance. The scope of the compliance must be provided. Any exceptions must be shared with the Authority. https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

2.3.2. Archive Services:

2.3.2.1. The provision of services to allow for the Authority's Data to be archived, retrieved, destroyed, and disposed of according to the Authority's data retention policies.

2.3.2.2. There is a potential to work with the authority and incumbent supplier to transfer archived data that is currently stored in IBM Spectrum protect to the supplier's chosen solution. The expectation is that this may not be required, however we would like an illustrative costed option.

2.4. Increase use of Cloud Computing

2.4.1. **We have an aspiration of migrating applications that are currently hosted in CHDC to our public cloud platforms. We would like the new supplier to support our migration roadmap and provide a rate card for the necessary resources that would be required to achieve this aim.**

2.4.2. **Supplier shall note that this requirement shall be delivered as an optional service and on an ad hoc basis dependent on the business roadmap for services and applications hosted in the CHDC.**

2.4.3. **For the avoidance of doubt, this service, if required, shall be delivered as work packages using Statement of Works (SOWs) and on Time and Materials or Capped Time and Materials basis, subject to the Authority internal approval process.**

2.5. Service Management Service

2.5.1. The Service Management Services shall integrate (i) the Hosting Services' and Technical Services' technical interfaces, processes, and data exchange with the (ii) Authority's ITSM.

2.5.2. Service Management Services will be facilitated using the Authority's ITSM Tool. Suppliers must utilise the Authority's ITSM Tool in delivering the Services.

2.5.3. In addition to standard ITIL processes, process descriptions/requirements at (i) to (xviii) have been included below for clarification, together with references to requirements in **Annex 2** as appropriate.

2.5.4. The Service Management Services also include the reporting requirements at paragraphs 45 to 48 of **Annex 2**.

2.5.5. Access Management

In addition to the standard ITIL Access Management process the following requirements apply:

Annex 2: paragraphs 1 to 3 inclusive.

2.5.6. Incident Management

In addition to the standard ITIL Incident Management process the following requirements apply:

Annex 2: paragraphs 4 and 5.

2.5.7. Problem Management

In addition to the standard ITIL Problem Management process the following requirements apply:

Minimisation of adverse effect on the Authority's Services of Incidents and Problems caused by errors in the infrastructure, and proactive prevention of the occurrence of Incidents, Problems, and errors.

Annex 2: paragraphs 6 and 7.

2.5.8. Request Fulfilment

In addition to the standard ITIL Request Fulfilment process the following requirements apply:

Annex 2: paragraphs 8 and 9.
Provision of channel(s) for End Users, authorised systems, and authorised processes to request and receive standard Operational Services for which a predefined approval and qualifications process exists.

2.5.9. Change Management

In addition to the standard ITIL Change Management process the following requirements apply:

Annex 2: paragraphs 10 to 15 inclusive.

2.5.10. Service Desk

The Authority will set up the Authority's Service Desk in accordance with standard ITIL Service Desk function.

The following requirements apply:

Annex 2: paragraphs 16 to 21 inclusive.

2.5.11. Service Catalogue

In addition to the standard ITIL Service Catalogue process the following requirement applies:

Annex 2: paragraph 22

2.5.12. Service Knowledge Management

The Authority will set up the Authority's SKMS in accordance with the standard ITIL Service Knowledge Management process.

The following requirement applies:

Annex 2: paragraph 2

2.5.13. Availability Management

In addition to the standard ITIL Availability Management process the following requirements apply:

Annex 2: paragraphs 24 and 25.

2.5.14. Event Management

In addition to the standard ITIL Event Management process the following requirements apply:

Annex 2: paragraphs 26 to 28 inclusive.

2.5.15. Capacity Management

In addition to the standard ITIL Capacity Management process the following requirements apply:

Annex 2: paragraphs 29 to 33 inclusive.

2.5.16. Demand Management

In addition to the standard ITIL Demand Management process the following requirements apply:

Annex 2: paragraphs 34 to 36 inclusive.

2.5.17. IT Service Continuity Management (ITSCM)

In addition to the standard ITIL Service Continuity Management process the following requirements apply:

Business Continuity and Disaster Recovery

2.5.18. Service Asset Configuration Management (SACM)

In addition to the standard ITIL Service Asset Configuration Management process the following requirements apply:

Annex 2: paragraphs 37 and 38.

2.5.19. Continual Service Improvement

In addition to the standard ITIL Continual Service Improvement process the following requirements apply:

Annex 2: paragraph 39 and 40.

2.5.20. Service Level Management

The Authority will set up service level Agreements within the Authority in accordance with the standard ITIL Service Level Management process.

In addition to the standard ITIL Service Level Management process the following requirement applies:

Annex 2: paragraph 41.

2.5.21. Release and Deployment

In addition to the standard ITIL Release and Deployment process the following requirements apply:

Annex 2: paragraphs 42 and 43.

2.5.22. Transition Planning and Support

In addition to the standard ITIL Transition Planning and Support process the following requirement applies:

Annex 2: paragraph 44.

2.6. Security Management

2.6.1. The supplier must comply with, and the supplier must evidence their compliance with the latest version of HMG cyber security strategy, NCSC standards and achieve ISO27001 certification for the scope of managed infrastructure services. Further information can be found in the ITT technical response envelope.

2.6.2. The scope of the compliance must be provided. Any exceptions must be shared with the Authority. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

2.6.3. The Authority's Information Governance requirements will be captured in the order form at attached to this ITT.

2.6.4. The Supplier shall provide an up-to-date contact to deal with any Information Security incidents that occur outside of normal business operation.

2.6.5. The Supplier shall respond to security alerts within agreed timescales.

2.6.6. The Supplier shall allow and facilitate the install and management of security monitoring software and security tooling software in active mode, provided and licenced by the NHS BSA.

2.6.7. The Supplier shall allow the NHS BSA to isolate services – infrastructure in the event of a major cyber security event via security tooling provided by the NHS BSA.

2.6.8. The Supplier shall collaborate with the NHSBSA Security operations team on the management of and outputs from IT Health Check tests, all ITHC are to be carried out by CHECK approved testers.

2.6.9. The Supplier shall provide a security compliance report to the Customer each Service reporting period.

2.6.10. The Supplier will provide an appropriate trained and competent representative to attend the Customer's Supplier Security Forum.

2.6.11. The Supplier shall notify the Customer immediately on becoming aware of a Major Security Incident and shall state the impact to the Customer. The Supplier shall follow NHSBSA security incident framework processes.

2.6.12. The supplier shall have appropriately cleared staff that are aligned to the principles set out in the HMG personnel Security controls,20221031-HMG Personnel Security Controls-V6.0-October 2022.docx (publishing.service.gov.uk)

2.6.13. The service provider must comply with the latest version of NCSC's Secure Design Principles. The scope of the compliance must be provided. Any exceptions must be shared with the Authority. https://www.ncsc.gov.uk/collection/cyber-security-design-principles

2.6.14. The service provider must comply with the latest version of NCSC's Secure system administration. The scope of the compliance must be provided. Any exceptions must be shared with the Authority. https://www.ncsc.gov.uk/collection/secure-system-administration

2.6.15. The service provider must complete the NCSC Cyber Assessment Framework (NCSC CAF guidance - NCSC.GOV.UK) and provide evidence in the attached XLS (Annex A).

2.7. Interface Requirements

2.7.1. The Supplier shall ensure that the integration between the Supplier Applications and Authority Applications (including between the Supplier's monitoring and management suite(s) is preserved during and after any new Releases or upgrades.

2.7.2. The Collaboration Agreement and the ITSM policies, processes and procedure documents set out the management obligations/responsibilities.

2.8. Other Authority Requirements

2.8.1. Architecture Requirements

2.8.1.1. Architecture documents and diagrams of the infrastructure must be created and updated when any changes occur.
2.8.1.2. This will need to identify where define BSA standards, patterns and policies are both adopted and deviated from.
2.8.1.3. Architecture Documents and Diagrams must use BSA Tools.
2.8.1.4. Architecture Documents and Diagrams must use BSA Documentation Standards.
2.8.1.5. The initial Design must be agreed with the NHSBSA Design Authority prior to implementation.
2.8.1.6. Any significant changes to the design must be agreed through the appropriate Architecture governance boards include NHSBSA Design Authority prior to implementation.
2.8.1.7. Provide reports providing insight into end-of-life products and services and progress on any agreed mitigation plans.

2.8.2. Social Value Requirements

2.8.2.1. The Authority requires the Supplier to deliver Social Value Initiatives throughout the life of the contract. As part of the response to this ITT, Supplier is expected to provide a method statement setting out its approach to Social Value throughout the life of the contract. This will be evaluated as part of the overall scoring of the bid responses.

2.8.2.2. In addition to providing the methodology, Supplier organisation is expected to provide commitments to Social Value and KPIs for reporting as part of the Contract Management Plan. These commitments shall be included in the Service Level schedule of the Call off Contract.

2.8.3. Modern Slavery Requirements

2.8.3.1. Supplier will be expected to support the Authority to prevent Modern Slavery and Human Trafficking by demonstrating what their organisation is doing in terms of prevention in their supply chain.

2.8.3.2. The intention is to use the Modern Slavery Assessment Tool (MSAT) available on Modern Slavery Assessment Tool - Supplier Registration Service (cabinetoffice.gov.uk)

2.8.4. Environmental Sustainability Requirements

2.8.4.1. The Authority requires the Supplier to support the Authority in protecting the environment: Delivering against our Net Zero target and, supporting a sustainable, healthier future for all.

2.8.4.2. Detailed requirements are captured in Annex 6.

Crown Commercial Service

Section 3 **Annexes**
Annex 1 **Crown Hosted Setup**

Datacentre Overview (November)

Spreadsheet below with Datacentre Hardware

DC Hardware.xlsx

[redacted]

- [redacted]
- [redacted]

[redacted]

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

Annex 2- Service Management Services Requirements
Access Management

1. The Supplier shall collaborate with the Authority to manage the lifecycle of End User accounts and associated Data/information in relation to the Operational Services.
2. The Supplier will provide multiple role-based access levels to the Operational Services for the Authority, the Supplier, and the Other Suppliers for the management of Operational Services in alignment with the Supplier User Access Control Policy.
3. The Supplier shall work with the Authority and Other Suppliers to support the Authority's requirements for multiple role-based access levels to the Operational Services.

Incident Management

4. The Supplier shall notify the Authority immediately on becoming aware of a Major Incident and shall state the impact to the Authority. The Supplier shall communicate this via a call as defined in the Authority's Major Incident process.
5. The Supplier shall provide early notification, as soon as is reasonably practical, to the Authority of any potential breach of Performance Indicators.

Problem Management

6. As soon as is reasonably practical the Supplier must provide information on Workarounds, Known Errors and Problems related to the Services for use by the Authority, Supplier or Other Suppliers in relation to Problem Management.
7. The Supplier will, where appropriate and possible, provide a proposal to the Authority in relation to Problem Management where the resolution is outside of the Services.

Request Fulfilment

8. The Supplier shall support the Authority and the Other Suppliers in the identification and resolution of conflicts which arise in the fulfilment of competing Service Requests in accordance with the ITSM documentation set.
9. Where the Supplier has multiple Service Requests which may result in breach of Performance Indicators the Supplier will take all reasonable steps to avoid the breach and if a breach remains likely, must notify the Authority in advance of the breach occurring.

Change Management

10. The Supplier shall perform an evaluation of both intended and unintended effects of a proposed Change or cross-functional Change if it affects the Authority's Services and shall provide such information to the Authority in accordance with the Change Management Process.

11. The Supplier shall maintain a matrix of nominated Supplier Approved Personnel who are authorised to request and to approve Changes and provide it to the Authority in time period so as to avoid impact to the Authority's ability to conduct its business.

12. The Supplier shall continue to propose Changes to the Operational Services for pre- approval by the Authority. Once pre-approved, each of these Changes shall become a Standard Change.

13. In relation to the Services the Supplier will, where required, provide an impact assessment and a proposal in relation to a Change proposed by the Authority or other Suppliers.

14. Where the Supplier initiates a Change to its integration with the authority's ITSM, the Supplier shall be responsible for any costs incurred by the Authority or Other Suppliers in considering, and if applicable, arising as a result of that Change.

15. Where there is a Supplier initiated Change to the Services which has no impact on the other Authority's Services it shall not be governed by the Authority's Change Management Process.

Service Desk

16. As soon as reasonably practicable, the Supplier shall inform the Authority's Service Desk of any Incident and its impact on any of the Authority's Services.

17. The Authority's Service Desk will operate a self-service portal. Under Continual Service Improvement the Supplier will continually propose and, if agreed by the Authority, implement, elements of Operational Services that can be delivered through the Authority's self-service portal to allow End Users to use certain elements of the Operational Services directly.

18. The Supplier shall provide Service-specific or Service-related Knowledge Articles to update the Authority's SKMS which is used by the Authority's Service Desk. The Supplier shall review these Knowledge Articles to ensure the currency of information every 6 (six) months or at another frequency agreed with the Authority.

19. In relation to the Services, the Supplier shall provide the Authority with such relevant information, training and training materials as may be required to enable the Authority's Service Desk to achieve or exceed its target of 50% (fifty percent) for contact resolution fix for Incident.

20. For all Service Management Services engagement, the Authority's Service Desk shall be the initial point of contact for the Supplier.

21. The Supplier shall provide to the Authority current and up-to-date contact details for all Supplier Approved Personnel. Changes to contact details shall be notified to the Authority within a time period that avoids impact to the Authority's ability to conduct its business.

Service Catalogue

22. The Supplier shall provide a Service Catalogue for the Operational Services, with prices derived from the tables in Schedule 7.1(Charges and Invoicing) and shall ensure the accuracy of that

Service Catalogue. If making Changes to its Service Catalogue, the Supplier shall comply with the Change Management Process and any other applicable provisions of the Call Off Contract.

Service Knowledge Management

23. The Supplier shall provide relevant Services data to the Authority, that following Authority approval, will be included in the Authority's SKMS to increase and/or improve End User self-service capability for Request Fulfilment and Incident Resolution.

Availability Management

24. The Supplier shall draw up and maintain a Maintenance Schedule and shall execute that Maintenance Schedule in accordance with Change Management Process.

25. The Supplier shall provide the Authority with a detailed impact assessment for any new or amended Availability requirements that the Supplier proposes for the Services. The Supplier shall do this under the Change Management Process.

Event Management

26. The Supplier shall deal with all Events. The Supplier shall report relevant details of Events to the Authority, including corrective actions taken, in a format agreed with the Authority, monthly or at another frequency agreed with the Authority.

27. In relation to the Services, the Supplier must immediately raise a single Incident record in the Authority's ITSM Tool for all Service-impacting correlated Events.

28. Event correlation activity is the sole responsibility of the Supplier. The Supplier shall carry out this Event correlation activity within its own tool and provide the correlated results to the Authority, in a manner agreed with the Authority.

Capacity Management

29. The Supplier shall propose Capacity solutions and options to allow the Authority to optimise Capacity decisions, including, where appropriate, options better to manage resource usage by e.g., changed use patterns.

30. The Supplier shall formally review Capacity requirements for its Services as part of the Authority's normal business planning cycle (which the Authority will make known to the Supplier).

31. The Supplier shall identify opportunities for optimising Capacity in its Capacity plans and recommend appropriate action to the Authority.

32. The Supplier shall proactively monitor Capacity and provide trend analysis to ITSM.

33. The Supplier shall operate and maintain a Capacity Management plan for the Services.

Demand Management

34. The Supplier shall collaborate with the Authority and the Other Suppliers in developing, agreeing, and implementing a Demand Management process for the Operational Services.

35. The Supplier shall maintain a knowledge base of past and current demand for the Services. The Supplier shall use the knowledge base to predict future demand and inform its Capacity plan. The Supplier shall provide such information to the Authority and in a format as is in each case agreed with the Authority during the Implementation Services, monthly or at such other frequency as is agreed by the Authority during the Implementation Services.

36. The Supplier shall collaborate with the Authority and the Other Suppliers to develop and implement strategies to manage unexpected demand and avoid adverse impact to the Authority's ability to conduct its business.

.

Service Asset Configuration Management (SACM)

37. The Supplier shall maintain Configuration Items (CIs) and Service Assets for the Services, and their constituent components as listed in its Service Catalogue. The Supplier shall record the relationships between the CIs. The Supplier shall update the Authority's Configuration Management System with all that information at the level of detail required by the Authority and shall ensure that such information is accurate and complete, and where necessary kept up to date.

38. The Supplier shall collaborate with the Authority and the Other Suppliers to maintain a Technical Dependency Register. This shall include compliance with the relevant provisions of the Collaboration **Call Off Contract**.

Continual Service Improvement

39. The Supplier shall collaborate with the Authority and the Other Suppliers in the delivery of the Continual Service Improvement Programme across the Authority's Services and shall contribute to the Continual Service Improvement Programme.

40. The Supplier shall support the Authority in the maintenance and improvement of the ITSM and ITSM processes to support the objectives of Continual Service Improvement. Changes shall be made using the Change Management Process and not the change procedure in Schedule 8.8 (Business Growth and Innovation Change Procedure) nor using the Contract Change Control Procedure.

Service Level Management

41. The Supplier shall collaborate with the Authority and the Other Suppliers to support the Authority's internal service level agreement (which the Authority will make available to the Supplier). The Supplier shall provide such reports to the Authority as the Authority may require for the purpose of determining whether the Authority has met the requirements in those internal service level agreements.

Release and Deployment

42. The Supplier shall provide the Authority with an annual Release schedule for the Services, in collaboration with the Authority and the Other Suppliers.

43. The details of the Release shall be provided in advance to the Authority in accordance with the Change Management Process.

Transition Planning and Support

44. The Supplier shall provide comprehensive documentation and transfer of knowledge to facilitate transition planning and support for all new or changed Services and shall provide them to the Authority in accordance with the Change Management Process

Reporting

45. The supplier shall attend monthly service Review meetings.

46. The Supplier shall provide the Authority with Management Information data in relation to the Services to support the Authority in the production of the Authority ITSM Reports, as agreed. ITSM reports should be provided to the authority 48 hours prior to the Service Review Meeting. The ITSM report should provide details of supplier compliance against the ITIL practices referenced above.

46. The Supplier shall continue to design and implement the Management Information data so that it continues to support the Authority's Management Information requirements.

47. The Supplier shall address and resolve any queries raised by the Authority with management data, Supplier Data and/or other data or reports provided by the Supplier.

48. The Supplier shall provide the Supplier Data to the Authority throughout the Contract, in a format and at a frequency agreed by the Authority. The Supplier shall demonstrate to the satisfaction of the Authority, on request by the Authority, that the Supplier Data has integrity, is accurate, complete, and not misleading.

Crown Commercial Service

Annex 3 RPO Objectives/BC

NHSBSA Prioritised Activities (Oct 2023)

Spreadsheet below with Prioritised Activities

NHSBSA Prioritised Activities Oct 23 upd

Crown Commercial Service

Annex 4 MIS Network Infrastructure

MIS Network Infrastrcuture Diagr

Crown Commercial Service

Annex 5 BSA Crown Parks Asset List

BSA Crown Parks Asset List with all available lifecycle dates:

BSA Crown Parks Asset List - with all av

Crown Commercial Service

Annex 6 Environmental Requirements

Managed Infrastructure Services

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

Not Applicable

Part B – Service Charges

Description	Cost
Operational Management of the Infrastructure Services as outlined in section 2.1 of the Statement of Requirement of the ITT- total cost over 2 years	[redacted]
Technical Services as outlined in section 2.3 of the Statement of Requirement of the ITT (backup cost per TB, based on 270TB- total cost over 2 years)	[redacted]
Service Management (required to manage the ITSM integration as outlined in section 2.5 of the Statement of Requirement of the ITT)- total cost over 2 years	[redacted]
Transition Management and Implementation (One-off)	[redacted]

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

Day Rate Card		
Role/Consulting Hierarchy	**Day Rate (ex VAT)**	**SFIA 8 Level of Responsibility**
Analyst	[redacted]	Follow
Junior Consultant	[redacted]	Assist
Consultant	[redacted]	Apply
Senior Consultant	[redacted]	Enable
Principal Consultant	[redacted]	Ensure, Advise
Managing Consultant	[redacted]	Initiate, Influence
Partner	[redacted]	Set Strategy, Inspire, Mobilise

Part D- Indexation

All costs under this contract shall be subject to indexation.

Where the Charges are stated to be "subject to Indexation" they shall be adjusted in line with changes in the Consumer Price Inflation (CPI) measure (as determined by the Office for National Statistics). All other costs, expenses, fees and charges shall not be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier.

Charges shall not be indexed during the first year following the Start Date.

Crown Commercial Service

Where a Charge is subject to Indexation then it will be applied annually on the first day of September. The first indexation will be applied from the first day of September 2025 and subsequent indexations will be on the first day of September in each subsequent year.

Where indexation applies the relevant adjustment shall be:

- determined by increasing or decreasing the relevant amount or sum by no more than the percentage change in the index.
- calculated by using the published index for the 12 months ended on the 31st of August immediately preceding the relevant Review Date.

The following CPI index will apply to the Charges.

Consumer price inflation tables - Office for National Statistics

Where the CPI index:

- is used to calculate the adjustment at Review Date that figure will be used as the baseline to calculate the following years adjustment.
- is no longer published, the Buyer and the Supplier shall agree a fair and reasonable replacement that will have substantially the same effect.

Part E- Invoicing and Payment Terms

1. Payments under this contract shall be made monthly in arrears
2. The Supplier shall prepare and provide to the Authority for approval of the format a template invoice within 10 Working Days of the Effective Date which shall include, as a minimum, the details set out in Paragraph 1.2 together with such other information as the Authority may reasonably require to assess whether the Charges that will be detailed therein are properly payable. If the template invoice is not approved by the Authority then the Supplier shall make such amendments as may be reasonably required by the Authority.
3. The Supplier shall ensure that each invoice contains the following information:

   (a) the date of the invoice;

   (b) a unique invoice number;

   (c) the Service Period or other period(s) to which the relevant Charge(s) relate;

   (d) the correct reference for this Agreement;

   (e) the reference number of the purchase order to which it relates (if any);

   (f) the dates between which the Services subject of each of the Charges detailed on the invoice were performed;

   (g) a description of the Services;

   (h) the pricing mechanism used to calculate the Charges (such as , Fixed Price, Time and Materials etc);

   (i) any payments due in respect of Achievement of a Milestone, including the Milestone Achievement Certificate number for each relevant Milestone;

   (j) the total Charges gross and net of any applicable deductions and, separately, the amount of any Reimbursable Expenses properly chargeable to the Authority under the terms of this Agreement, and, separately, any VAT or

other sales tax payable in respect of each of the same;

(k) details of any Service Credits or Delay Payments or similar deductions that shall apply to the Charges detailed on the invoice;

(l) reference to any reports required by the Authority in respect of the Services to which the Charges detailed on the invoice relate (or in the case of reports issued by the Supplier for validation by the Authority, then to any such reports as are validated by the Authority in respect of the Services);

(m) a contact name and telephone number of a responsible person in the Supplier's finance department in the event of administrative queries; and

(n) the banking details for payment to the Supplier via electronic transfer of funds (i.e. name and address of bank, sort code, account name and number).

4. Each invoice shall at all times be accompanied by Supporting Documentation. Any assessment by the Authority as to what constitutes Supporting Documentation shall not be conclusive and the Supplier undertakes to provide to the Authority any other documentation reasonably required by the Authority from time to time to substantiate an invoice.
5. The Supplier shall submit all invoices and Supporting Documentation to:

   Finance Department
   NHS Business Services Authority
   Stella House
   Goldcrest Way
   Newcastle upon Tyne
   NE15 8NY

   with a copy (again including any Supporting Documentation) to such other person and at such place as the Authority may notify to the Supplier from time to time.

6. All Supplier invoices shall be expressed in sterling or such other currency as shall be permitted by the Authority in writing.
7. The Authority shall regard an invoice as valid only if it complies with the provisions of this Part E. Where any invoice does not conform to the Authority's requirements set out in this Part E, the Authority shall promptly return the disputed invoice to the Supplier and the Supplier shall promptly issue a replacement invoice which shall comply with such requirements.
8. If the Authority fails to consider and verify an invoice in accordance with paragraphs iv and vii the invoice shall be regarded as valid and undisputed for the purpose of paragraph 2.1 (Payment in 30 days) after a reasonable time has passed

Payment Terms

i. The Authority shall make payment to the Supplier within 30 days of verifying that the invoice is valid and undisputed.

ii. Unless the Parties agree otherwise in writing, all Supplier invoices shall be paid in sterling by electronic transfer of funds to the bank account that the Supplier has specified on its invoice.

Crown Commercial Service

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)

Not Applicable

Crown Commercial Service

Attachment 3 – Supplier Solution and Implementation Plan

1. Introduction

1.1. Service Overview

NHSBSA (the Authority) require a further period of managed services related to NHSBSA private cloud assets in Crown Hosting data centres.

The period is for two years, with two optional 12-month extensions (2+1+1)

Additionally, NHSBSA will require services relating to environment and social value and may wish to draw upon further optional services. These are set out below.

Start date August 22nd, 2024. Transition activity will be required, this is detailed to the extent it has been defined so far.

1.2. Background & Context

NHSBSA has employed Agilisys as its Managed Infrastructure Service partner for the last 6 years. NHSBSA are now in-sourcing some of the services currently provided, and the services from 22 August 2024 will have a significantly reduced scope from current service provision. A new procurement for the service provision beyond 22nd August was started in 2023. This document describes the solution proposed by Agilisys in response to that procurement.

2. Description of Services

2.1. Supplier Solution

Agilisys will provide

(1) Hosting management, including patch management
(2) Technical services, including backup, recovery and archive management
(3) Security management, including vulnerability management
(4) Service management in relation to (1), (2) and (3)

Service hours are 7am to 6pm, Monday to Friday excluding English bank holidays. Calls may be logged with Agilisys Service Desk 24 hours / 7 days and will be actioned during working hours.

Agilisys will also make available professional services teams to support or lead projects relating to cloud innovation and migration activities, as agreed by NHSBSA and Agilisys from time to time, subject to quotation and change control.

Agilisys will support NHSBSA with reporting on social value and environmental impact.

2.1.1 In Scope

The following services are in scope of the Services.

2.1.1.1 Hosting management

NHSBSA has elected to provide hardware and premises, maintenance contracts, software licensing etc., so that the role of Agilisys will be to providing management only. Scope of the service provided by Agilisys is

hosting management of Windows, Linux and Unix equipment in the two Crown Hosting Data Centres, at Spring Park and Cody Park. Services included are:

- Patch and Vulnerability Management
- Physical Infrastructure Management
- Business Continuity and Disaster Recovery
- Recovery testing
- Server, storage, core network and firewall management
- Acting upon relevant security alerts
- Provision of a self-service capability for VMware hosted services

The provision of the overall infrastructure service is divided between NHSBSA and Agilisys. The split of responsibilities is summarised in the diagram below and covered in section 2.14 of this document.

Figure 1 - Service Overview

2.1.1.2 Patch and Vulnerability Management

Agilisys will implement version and point upgrades to maintain infrastructure services within Supplier and Vendor lifecycles. Through our Product Lifecycle process, we track the published upgrades of hosting, OS and Firmware that is being used in managed environments. We will establish an ongoing maintenance schedule including all patching and agree this with the Authority. Patching and the lifecycle status of products will be reported at regular governance meetings.

We use [redacted] to manage Patching systems, with updates managed through [redacted]. Updates will be deployed in a phased manner, starting with management systems, through dev and test to non-critical systems, finally critical systems. This provides an opportunity to identify issues with patches prior to patching Line of Business Systems (LoBS).

Solaris systems will be patched according to a separate, agreed, schedule.

Our processes adhere to National Cyber Security Centre (NCSC) recommended timelines for patching, ie high and critical vulnerabilities to be patched within 14 days. Critical zero-day vulnerabilities will be patched as soon as reasonably practical, subject to vendor release and approval by NHSBSA.

Our service model will use [redacted].

[redacted] will maintain an inventory of assets and associated patching status, including any exceptions that are not be patched. Patching levels within the estate will be reported on a monthly basis, during scheduled governance meetings.

2.1.1.3 Backup, recovery and archive management

Scope of the service provided by Agilisys for backup, recovery and archive management is:

- licensing of [redacted]
- management of that system, including monitoring and periodic Business Continuity restoration testing to an agreed schedule.

[redacted]

2.1.1.4 Service Management

Scope of the service provided by Agilisys for Service Management is aligned to ITIL4 processes in respect of hosting, backup, recovery and archive services described above. The following will be provided:

- **Incident Management** - coordinated through our Agilisys Service Centre and will use the Authority's IT Service Management (ITSM) Tool to manage incidents.
- **Major Incident Management** – Agilisys is not providing a Major Incident Management service. However, Agilisys will participate in NHSBSA-led major incident activity during work hours and will follow NHSBSA Cyber Incident Response Process (CIRP). Out of hours, NHSBSA should contact Agilisys service desk in the event of a major incident.
  Please note, Agilisys, at its own discretion, may choose to assign a major incident manager from time to time to support its response to major incidents.
- **Problem Management** - working alongside the Authority to highlight, investigate, and communicate Workarounds, Known Errors and Problems.
- **Request fulfilment** - Agilisys will manage and track Service Requests and Changes through the Authority's ITSM Tool.
- **Change Management** - Agilisys will attend the Authority's Change Authority Board and perform evaluation of both intended and unintended effects of any relevant, proposed Change.
- **Agilisys Service Desk** – will act as the coordination point for the Authority for all Incidents and Requests.
- **Service Catalogue** – shall be provided for standard services.

- **Service Knowledge Management** – Agilisys will provide content related to the Services, and review information to be included in the Authority's Service Knowledge Management System (SKMS), on request.
- **Availability Management** – Agilisys will agree and deliver the Services in accordance with a Maintenance Schedule that will be reviewed and managed though the appropriate governance meetings.
- **Event Management** – Agilisys will use [redacted] to identify issues; deal with Events and report relevant details to NHSBSA.
- **Capacity & Demand Management** – Agilisys will monitor the utilisation and capacity of the managed systems and make optimisation recommendations
- **Service Continuity** – Agilisys will develop a Business Continuity Plan for the Services and agree this plan with the Authority. The Plan will include a schedule of periodic testing that will be conducted as agreed with the Authority.
- **Service Asset Configuration Management** - Agilisys will maintain Configuration Items (CIs) and Service Assets for the Services and maintain an Asset Register of the supported services for the Authority.
- **Continual Service Improvement** - our Service Manager will work with the Authority to identify opportunities for Continual Service Improvement and implement initiatives agreed with the the Authority.
- **Service Level Management** - Agilisys will collaborate with the Authority and the Other Suppliers to support delivery of the Services to the Service Levels. Where Service Levels are at risk, the Agilisys Service Manager will coordinate resources to mitigate the risk, and in all cases, will notify NHSBSA if Service Level failure occurs or becomes likely.
- **Release and Deployment** - Agilisys will ensure that releases are managed smoothly, ensuring stability, reliability, and increased efficiency, minimising issues, and maintaining service stability.
- **Transition Planning** - Agilisys will maintain documentation regarding the services throughout the contract term and will make these available to the Authority on request.
- **Performance Monitoring and Compliance** - Agilisys will produce performance and compliance reporting monthly, with data drawn from [redacted]

2.1.1.5 IT Service Management Tooling

Agilisys and the Authority aim to connect their respective ITSM tools. The timing and mechanism for doing so will be determined when the Authority's ITSM tool re-procurement plans are complete and Agilisys has migrated resolver groups delivering the Services onto its new [redacted] Service Management tool. NHSBSA and Agilisys agree that flexibility will be required to determine the best approach as the contract unfolds, to avoid wasting effort on connecting tools which may have a short life.

Until these two new ITSM tools are available, Agilisys will follow the currently established approach for Incident and Request Management, i.e.:

- Infrastructure alerts will be logged in Agilisys ITSM tool, and P1 incidents will be uploaded to the Authority's ITSM tool, informing the Authority's Service Desk.
- Outputs from the Agilisys-implemented Vulnerability Management tool will be captured in the Agilisys ITSM tool for remediation and summarised in a monthly report to the Authority.
- Threat Intelligence will be shared by NHSBSA with Agilisys upon NHS BSA being notified and Agilisys will assess if the threat/vulnerability is applicable to the CHDC environments.
- Service Requests will be managed in NHSBSA [redacted]
- Agilisys will provide a monthly report to the Authority detailing all non-P1 incidents raised and closed during the period.

The process will change for Infosec alerting, since these will now be routed to NHSBSA SIEM and triaged to Agilisys where appropriate. See diagrams below:

Infrastructure Event

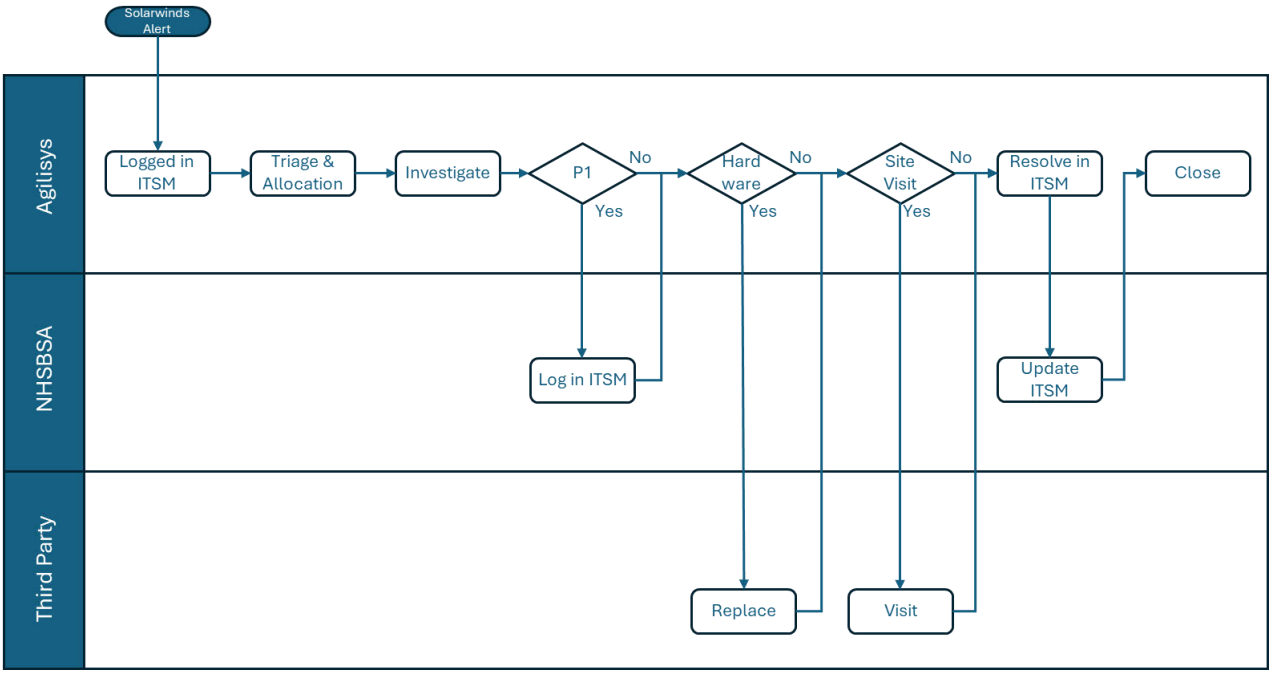

Figure 2 - Infrastructure Event Flow

Service Request – omitting Third Parties for simplicity

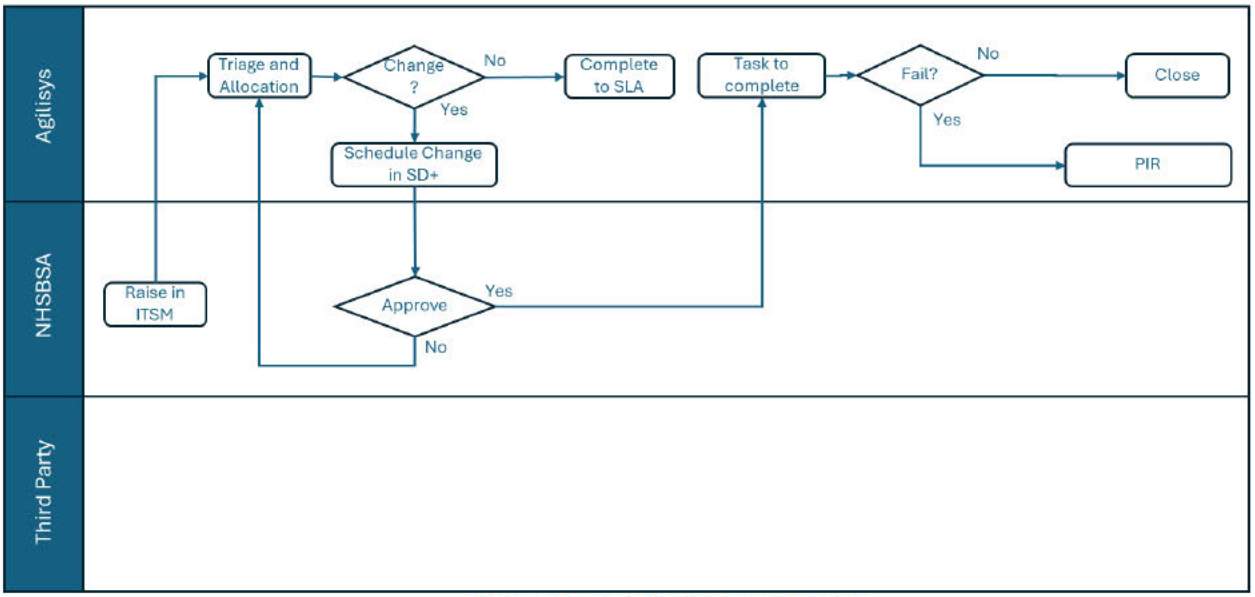

Figure 3 - Service Request Flow

[redacted]

Vulnerability Management

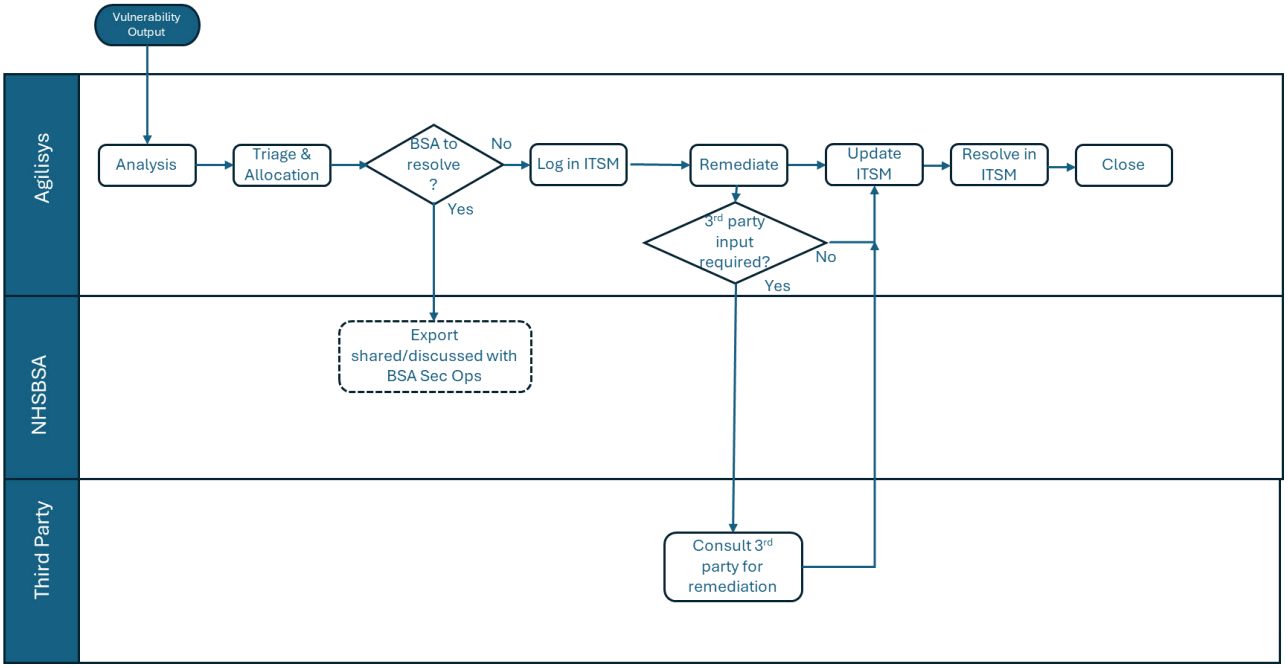

Figure 6 – Vulnerability Management Flow

2.1.1.6 Environmental and Social Value

Scope of the services provided by Agilisys in relation to environmental sustainability will be reporting on:

- Emissions associated with delivering the services
- Emissions associated with the grid electricity and standby power in Crown Hosting
- Annual report on the Agilisys Carbon Reduction Plan

Scope of the services provided by Agilisys in relation to social value will be reporting on:

- Absolute number of hires with incomplete employment checks.
- Gender pay gap metrics

Agilisys additionally commits to the Modern Slavery Act throughout the life of the contract. To this end, Agilisys:

- shall not use, nor allow its subcontractors to use, forced, bonded or involuntary prison labour
- shall not require any employees or the employees of any subcontractors to lodge deposits or identity papers with their employer and shall be free to leave their employer after reasonable notice
- warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world

- warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world
- shall make reasonable enquiries to ensure that its officers, employees and subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world
- shall have and maintain throughout the Term its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and include in its contracts with its sub-contractors anti-slavery and human trafficking provisions
- shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under the Contract
- shall comply with the request by the Authority to complete the Modern Slavery Assessment Tool within sixty (60) days of commencement of the contract
- shall work in good faith with the Authority to work on the recommendations generated from the responses to the MSAT and report on improvements on a quarterly basis
- shall notify the Authority as soon as it becomes aware of any actual or suspected slavery or human trafficking in a supply chain which has a connection to this contract

2.1.2 Optional Services

The following services are optional, and are available for the Authority to draw down, subject to impact assessment, quotation and Change Control.

2.1.2.1 Local Server Room Backup

Optionally, the Authority may use [redacted] capacity for LSR backups, provided:

a) there is sufficient unused licence capacity in the [redacted]
b) the Authority procures a backup management service for LSRs from Agilisys for the same period as licensing is required ([redacted] permit the resale of licenses without additional service provision)
c) [redacted] is provided on an annual basis from 1st January each year
d) [redacted] beyond year two of the contract is subject to change.

2.1.2.2 [redacted] Backup Implementation

[redacted]

- [redacted]
- [redacted]

2.1.2.3 Professional Services

Scope of the services provided by Agilisys in relation to Professional Services will be determined through Statements of Work as agreed from time to time between NHSBSA and Agilisys.

2.1.3 Out of Scope

The following items are out of the scope:

Ref	Description
1	Services not listed as being in scope (above), including all services to be exited by 22nd August such as hosting on Amazon Web Services, management of cloud consumption payments etc.
2	Termination Assistance and Exit activities delivered through the previous Managed Infrastructure Services contract
3	Provision of licensing and maintenance contracts, other than [redacted]
4	Provision of hardware. All equipment required to operate hosting and backup services will be provided by NHSBSA.
5	Security Operations Centre and SIEM. These are to be provided by NHSBSA. For clarity: Agilisys will facilitate running of [redacted] machines and making available of logs to NHSBSA SIEM. NHSBSA SOC will triage events and pass information relating to Agilisys services back to Agilisys. This is as shown in flowchart Figure 5 above. Hardware vulnerability scanning remains in Agilisys scope, see flowchart Figure 6 above.
6	Out of Hours service, ie weekends, bank holidays and outside of working hours of 7am to 6pm. Any out of hours service other than patching within Agilisys agreed maintenance window will be subject to availability of Agilisys staff at the time, to be confirmed on request, and will incur additional charges.
7	Provision of supplementary backup facilities, eg via MAB
8	Provision of Witness Server (unless otherwise commissioned)
9	Provision of LSR backups unless agreed via Contract Change

2.1.4 Roles and Responsibilities in Service Delivery

Agilisys will depend on services provided by the Authority to deliver the Services, these are detailed in the table below.

Service Element – Hosting Management	Authority Role	Agilisys Role
Infrastructure and management	• Provide all platform hardware, including Management environment, [redacted] and fabric, firewalls and network connectivity • Enable administrative and physical access to the Authority infrastructure, software, services, hosting racks, build rooms and working spaces within the Parks – unescorted access 24x7 for named Agilisys staff. • Provide [redacted] and licence. • Provide appropriate login credentials to all relevant systems	• Manage development, testing and production environments • Manage availability and capacity • Provide platform services i.e. server builds, web hosting platform services, high availability services, database services, virtualization services, storage management • Provide NHSBSA with a Self-Service capability for [redacted] environment only
Third party maintenance contracts and licensing/subscriptions	• Provide all licences and maintenance contracts except where noted • Ensure vendors are aware that Agilisys is appointed as NHSBSA's agent to operate the equipment and has access to vendor support • Provide maintenance contracts to include all provided infrastructure and licensing including, but not limited to, [redacted] required under the Services. • Licensing/subscriptions to cover [redacted].	• Provide licensing for: ○ [redacted] • Draw down services of third-party vendors as the Authority's agent as required

Service Element – Hosting Management	Authority Role	Agilisys Role
Performance of third party maintenance and licenced products	• Remediate any material underperformance by Authority-provided third party products and services • Raise and manage calls with Authority third-party providers in accordance with the Services, where the Authority has not provided the access for Agilisys to engage relevant third-parties. • Stop the clock for SLAs where Agilisys has correctly passed a call through to the Authority's third-party provider.	• Raise and manage calls with Authority third-party providers in accordance with the Services, where the Authority has provided the access for Agilisys to engage relevant third-parties. • Alert NHSBSA of material underperformance of NHSBSA-provided third party products and services
Patch and Vulnerability management	• Provide a dedicated [redacted] Agilisys to deploy its management systems in accordance with the Services.	• Deploy the requisite management systems within the dedicated [redacted] to an agreed schedule • Maintain the inventory of assets, patch status and ongoing maintenance schedule, and report monthly on these.
Security tooling and monitoring	• Provide [redacted] • Provide appropriately triaged alerts from the Authority's Security Operations Centre to the Agilisys Service Desk	• Make [redacted] available to NHSBSA SIEM • Act upon NHSBSA SOC alerts pertaining to Crown Hosting • Baseline metrics and alerting levels with [redacted] • Scan for vulnerabilities [redacted]; report and remediate as appropriate.
Business Continuity and Disaster Recovery	• Agree and support the recovery testing schedule • Conduct the actions for recovery testing as detailed within the recovery testing schedule	• Maintain the existing [redacted] backup solution for systems hosted within the Parks, with recovery testing and reporting to an agreed schedule
LAN and Firewall services	• Provide hardware, licensing and third-party maintenance and support as noted above	• Monitor network performance • Manage network and firewall configurations • Provide [redacted]

Service Element – Backup, Archive & Recovery	NHSBSA Role	Agilisys Role
Infrastructure and management	• Provide all platform hardware, including Management environment, [redacted], firewalls and network connectivity • Enable administrative and physical access to the Authority infrastructure, software, services, hosting racks, build rooms and working spaces within the Parks – unescorted access 24x7 for named Agilisys staff. • Provide [redacted] and licence. • Provide appropriate login credentials to all relevant systems	• Manage development, testing and production environments • Manage availability and capacity • Provide platform services i.e. server builds, web hosting platform services, high availability services, database services, virtualization services, storage management Provide NHSBSA with a Self-Service capability for [redacted] environment only
Licensing	• Advise Agilisys of changes to requirement for [redacted], if any. Changes must be communicated by 30th August to take effect from the following 1st January.	• Arrange annual [redacted] to the required level of 270TB.
Backup, Recovery and Archive service		• Maintain the existing [redacted] solution in Crown Hosting environment, in keeping with relevant guidance • Provide a Self-Service capability for backup restoration
Business Continuity and Disaster Recovery	• Define and support the recovery testing schedule	• Deliver recovery testing and reporting to an agreed schedule

Service Element – IT Service Management	NHSBSA Role	Agilisys Role
ITSM Tooling	• Collaborate to connect Agilisys and NHSBSA respective service management tools	• Collaborate to connect Agilisys and NHSBSA respective service management tools
ITIL service processes	• Take the lead role for service management on behalf of NHSBSA	• Respond to NHSBSA and support ITIL processes where they relate to hosting management and backups in Crown Hosting Data Centres
Reporting		• Provide the agreed reporting, see section 2.21

Service Element – Security	NHSBSA Role	Agilisys Role
IT Health Checks	• Facilitate access to enable IT health checks to take place	• Provide appropriate resources for delivery against agreed Statements of Work

Service Element – Security	NHSBSA Role	Agilisys Role
Security Compliance Report	• Provide appropriate input to process, and source data as needed	• Prepare report monthly
Supplier Security Forum	• Provide appropriate input to process	• Attend monthly
ISO270001	• Provide appropriate input to process	• Share evidence of certification

Service Element – Additional and Optional Services	NHSBSA Role	Agilisys Role
Cloud Innovation and Migration services	• Define requirements for innovation and migration services to enable agreement on Statements of Work	• Provide appropriate resources for delivery against agreed Statements of Work
Social Value – Method and Reporting		• Report on workplace inequality measures and continue to drive company policy. See also Reports section.
Modern Slavery		• Complete the online MSAT • Comply with regulations and company policy
Environmental Sustainability - Reporting		• Report on environmental metrics and continue to drive company policy. See also Reports section.

2.2 Transition Approach

Transition activities have been identified to help the service move from the outgoing contract to the new contract.
These will take place potentially before the new contract begins, and comprise:

- Complete the roll-out of [redacted] make logs available to NHSBSA SIEM
- Phased switchover from [redacted]
- Set up of NHSBSA [redacted] to enable Agilisys to manage assets under NHSBSA tenancy
- Enhanced infosec support and advisory through the transition period
- Provision of dedicated laptops – shared project between NHSBSA and Agilisys
- Training of appropriate NHSBSA employees to be able to switch off [redacted] in case of incidents out of hours

2.2.1 Timeline

The below timeline shows the timeline and duration of transition activities.

2.2.2 Activities & Deliverables

The below table defines the activities, deliverables, and acceptance criteria.

Ref	Activity	Deliverable	Acceptance Criteria
D-01	Transition activity	To be agreed in a Statement of Work re Transition Services	See Statement of Work re Transition Services
D-02	Professional services and third party passthrough Cloud Migration and other innovation activities	As set out in Statements of Work agreed by NHSBSA and Agilisys under this contract	As set out in Statements of Work agreed by NHSBSA and Agilisys under this contract

2.3 Governance

The project governance framework is based on the governance reports, artefacts and meetings set out below.

2.3.1 Reports and Artefacts

Artefact	Frequency	Purpose	Prepared by
Service Management report	Monthly	Assurance re SLA performance: • Service availability 99.5% • Resolution time for P1, 100% within 2 hours • Resolution time for P2, 100% within 4 hours • Resolution time for P3, 95% within 8 hours Completion time for urgent service request, 95% within 24 hours	Agilisys Service Management

Contract Change Control	Adhoc	**Contract Change Control** Contract Change Notice (CCN) used to agree a major variation to the scope, timelines, or charges.	Agilisys Account Manager
Project Change Control	Adhoc	**Project Change Control** Project Change Notice (PCN) used to agree minor changes within pre agreed tolerances to the scope, timelines, or charges.	Agilisys Account Manager
Ops Board Pack	Monthly	Status of overall programme.	Agilisys Account Manager
RAID Log	Live	Ensures tracking and management of Risks, Assumptions, Issues and Dependencies.	Agilisys Project Managers
Capacity Report	Quarterly	Review of capacity information	Agilisys Operations
TSM Report	Monthly	Backup performance to include: - Backup exceptions - Backup completion - Results of scheduled restoration testing - Utilisation of licensing	Agilisys Operations
Security Metrics/Compliance report	Monthly	To report the key information security metrics and incidents/events	Agilisys Information Security Manager
Workplace Inequality	Annually	Report on progress with workplace inequality measures	Agilisys Account Manager
Environmental Sustainability	Annually	Report on progress with environmental sustainability measures	Agilisys Account Manager

2.3.2 Governance Meetings

Meeting	Frequency	Purpose	Attendees
MIS Update	Weekly	Status review. Escalations if required.	Head of Tech and Cyber Infrastructure Manager Account manager
Operational Board	Monthly	Review programme status, RAID, contractual matters etc	As above plus Service Manager, SIAM, Commercial
Service Management Board	Monthly	Review of service levels and actions	Service Manager SIAM Infrastructure Manager
Partnership Board	Quarterly	Steering re status and innovation	CDDaTO Head of Governance Head of Tech and Cyber Commercial Account Manager
Supplier Security Board	Monthly	To discuss the key information security metrics and incidents/events	Information Security Manager – Agilisys BSA Cyber/Information Security leads

2.4 Risks

A risk log will be maintained throughout the contract and tracked as part of the governance process. All Operational risks will be managed through that process and they will not be discussed further here. The following key risks have been identified at the outset of the contract.

Ref	Risk	Probability	Impact	Mitigation	Owner
R-01	Process failure or poor user experience due to incomplete handover of responsibilities	Medium	Medium	Attention to new process flows; communication to wider stakeholders.	NHSBSA
R-02	Transition activities re MS Defender not completed in time	Medium	High	Increased frequency of check-in through transition period	Joint

2.5 Assumptions

The project approach, timelines and charges have been based on the following assumptions.

Ref	Title	Description
A-01	Acceptance Process	The Customer will provide timely input, review, and acceptance of the deliverables in accordance with the Acceptance Criteria.
A-02	Documentation	Documentation deliverables will undergo one review cycle and the Customer will provide feedback in a single document within 5 working days. Within 5 working days of Customer feedback, Agilisys will issue an updated document incorporating the agreed changes. This document constitutes the final accepted deliverable, and any further review cycles will be treated as a contract change control.
A-03	Personal Data	No personal data will be processed pursuant to this SoW/Proposal. If personal data may be processed during the project the Authority will ensure that it is supported by a relevant data processing impact assessment prior to any data processing occurring.
A-04	Timeline	The timeline in the Proposal assumes that services will be delivered on a continuous basis. Any extensions or standstill periods will be treated as a contract change control.
A-05	Charges	Charges shall be adjusted annually in line with Master Service Agreement/Head Contract indexation rules as appropriate.
A-06	Backup licence	It is assumed that 270TB will remain adequate licensing for NHSBSA
A-07	Managed Services	Management of hosting, backup etc is for a fixed fee. Any material change in fees or responsibilities outside of those described in this document will be subject to Change Control.
A-08	Professional Services	Professional services for cloud migration, innovation etc will be made available on a Time and Materials basis.

If any of the assumptions prove to be invalid or incorrect this may impact the timescales, quality or charges contained in this SoW/Proposal and Agilisys will be entitled where applicable to a reasonable extension of time, recovery of additional costs, performance relief and, where a resolution cannot be reached, may reasonably suspend delivery of the programme.

2.6 Customer Responsibilities

The Customer is responsible for the timely fulfilment of the following Customer Responsibilities.

Ref		Description

CR-01	Transition	See Customer Responsibilities in Statement of Work re Transition
CR-02	Contract Delivery	NHSBSA responsibilities as set out in section 2.14 of this document

Attachment 4 – Service Levels and Service Credits

Performance Levels

1. DEFINITIONS

In this Schedule, the following definitions shall apply:

"Available"	has the meaning given in Paragraph 1.1 of Part II of Annex 1;
"ITIL Change Request"	as defined under ITIL;
"Configuration Item"	is as defined under ITIL;
"Configuration Management System"	is as defined under ITIL;
"End User"	any person authorised by the Authority to use the IT Environment and/or the Services;
"Expected Service Uptime"	means the time that the Services are expected to be available to End Users, that is Monday to Sunday inclusive (including Bank Holidays) from 00:00 to 23:59.
"Major Incident"	is as defined under ITIL;
"Major Incident Report"	means the report produced by the Supplier as a Major Incident is closed defining the reason and resolution of the incident;
"Maximum Completion Time"	means the maximum time the Supplier is allowed in which to deliver the requirements of a Service Request as detailed in paragraph 4 of Annex 1 Part II of this Schedule;
"Maximum Resolution Time"	means the maximum time the Supplier is allowed in which to resolve a Service Incident as detailed in paragraph 3 of Annex 1 Part II of this Schedule;
"Negative Service Points"	means the deduction in Service Points given to the Supplier where the Supplier has performed above the Target Performance Level of a Key Performance Indicator;
"Performance Monitoring Report"	has the meaning given in Paragraph 1.1(a) of Part B;

“Performance Review Board”	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Agreement, as further described in Paragraph 1.5 of Part B;
“Repeat KPI Failure”	has the meaning given in Paragraph 3.1 of Part A;
“Root Cause Analysis”	is as defined under ITIL;
“Root Cause Analysis Report”	means the report produced by the Supplier after an incident has been resolved;
“Satisfaction Survey”	has the meaning given in Paragraph 5.1 of Part II of Annex 1;
“Service Availability”	has the meaning given in Paragraph 2 of Part II of Annex 1
“Service Boundary”	means any time during an incident or when fulfilling a Service Request where activities to fix or fulfil are not within the scope of the Services;
“Service Downtime”	any period of time during which any of the Services are not Available; and
“Service Request”	is as defined under ITIL;
"Supplier's Support Function"	the single point of contact set up and operated by the Supplier for the purposes of this Agreement;
“System Response Time”	has the meaning given in Paragraph 2.1 of Part II of Annex 1; and
“Unavailable”	in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available.

PART A: PERFORMANCE INDICATORS AND SERVICE CREDITS

1 PERFORMANCE INDICATORS

1.1 Annex 1 sets out the Key Performance Indicators and Subsidiary Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier. Annex 1 Part II also includes certain other performance procedures which the Supplier has agreed to perform in order to assist in meeting the Performance Indicators.

1.2 The Supplier shall monitor its performance against each Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B.

1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5.

2 SERVICE POINTS

2.1 If the level of performance of the Supplier during a Service Period equals the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

2.2 If the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraph 2.3.

2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in Annex 1 depending on whether the KPI Failure is a Minor KPI Failure, a Serious KPI Failure or a Severe KPI Failure, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 3.2 shall apply.

2.4 If the level of performance of the Supplier during the Service Period is above the Target Performance Level in respect of a Key Performance Indicator, Negative Service Points, where applicable, shall accrue to the Supplier in respect of that Key Performance Indicator.

2.5 The total Service Points applied to the Supplier for the Service Period is the Service Points less any Negative Service Points for each KPI measured for the Service Period.

2.6 Negative Service Points shall only apply to the Service Period in which they are accrued and shall not be carried forward to any subsequent Service Period. **Worked Example:**

Service Availability Severity Levels	**Service Points**
Above 99.5%	**-1**

Service Availability Severity Levels	Service Points
Target Performance Level: 99.5% Minor	0
KPI Failure: 99.0% - 99.4%	1
Serious KPI Failure: 98.0% - 98.99%	2
Severe KPI Failure: 97.5% - 97.99%	3
KPI Service Threshold: below 97.5%	4

Severity Incidents Severity Levels	Service Points
Above 95.0%	-1
Target Performance Level: 95.0% Minor	0
KPI Failure: 92.5% - 94.9%	1
Serious KPI Failure: 91.5% - 92.49%	2
Severe KPI Failure: 90.0% - 91.49%	3
KPI Service Threshold: below 90.0%	4

If in a given Service Period in respect of the Key Performance Indicators, a Supplier has achieved:

- *Service Availability of 99.9%*
- *Resolution Time for Severity 2 Incidents of 90% Resolution Time for Severity 4 Incidents of 95% where the Target Performance Level is 95%*

Service Points accrued for each Key Performance Indicator will be:

- *Service Availability accrues -1 Service Points as performance was above the Target Performance Level*

- *Resolution Time for Severity 2 Incidents accrues 2 Service Points as performance was a Serious KPI Failure*

- *Resolution Time for Severity 4 Incidents accrues 0 Service Points as performance was equal to the Target Performance Level*

Total Service Points accrued for the Service Period will be calculated as follows:

-1 + 2 + 0 = 1 Service Point

2.7 In calculating the total Service Points for the Service Period the value of the total. Service Points will never result in a value below zero.

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES

Repeat KPI Failures

3.1 If a KPI Failure occurs in respect of the same Key Performance Indicator in any period of two consecutive months, the second and any subsequent such KPI Failure shall be a **"Repeat KPI Failure"**.

3.2 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be the number of Service Points that would normally accrue in respect of an initial failure of that Key Performance Indicator multiplied in accordance with the following table:

Number of Repeat Failures	**Multiplier**
0 (initial failure)	1
1st repeat	2
2nd repeat	3
3rd and each subsequent repeat	4

SP = P x M

where:

SP = the number of Service Points that shall accrue for the Repeat KPI Failure;

P = the applicable number of Service Points for that KPI Failure as set out in Annex 1 depending on whether the Repeat KPI Failure is a Minor KPI Failure, a Serious KPI Failure, a Severe KPI Failure or a failure to meet the KPI Service Threshold.

and

M = the multiplier for the number of repeat failures as shown in the above table.

Worked example:

Service Availability Severity Levels	Service Points
Above 99.5%	-1
Target Performance Level: 99.5% Minor	0
KPI Failure: 99.0% - 99.4%	1
Serious KPI Failure: 98.0% - 98.99%	2
Severe KPI Failure: 97.5% - 97.99%	3
KPI Service Threshold: below 97.5%	4

Example 1:

If the Supplier achieves Service Availability of 98.5% in a given Service Period, it will incur a Serious KPI Failure for Service Availability in that Service Period and accordingly accrue 2 Service Points.

If, in the next Service Period, it achieves Service Availability of 97.6%, it will incur a Severe KPI Failure and accordingly accrue 3 Service Points, but as the failure is a first Repeat Failure, the Service Points accrued are multiplied by 2. (i.e. SP = 3 x 2).

If in the next Measurement Period it achieves Service Availability of 97.5%, it will again incur a Severe KPI Failure and according accrue 3 Service Points, but as this is a second Repeat Failure the Service Points accrued are multiplied by 3 (ie SP = 3 x 3).

3.3 If in any six (6) consecutive Service Periods a Supplier incurs 3 Repeat KPI Failures for the same Key Performance Indicator this will be deemed to be a Unacceptable KPI Failure.

Related KPI Failures

3.4 If any specific Key Performance Indicators refer to both Service Availability and System Response Times, the System Response Times achieved by the Supplier for any period of time during a Service Period during which the relevant Service or element of a Service is determined to be Non-Available shall not be taken into account in calculating the average System Response Times over the course of that Service Period. Accordingly, the Supplier shall not incur any Service Points for failure to meet System Response Times in circumstances where such failure is a result of, and the Supplier has already incurred Service Points for, the Service being Non-Available.

4 PERMITTED MAINTENANCE

4.1 The Supplier shall be allowed to book, with the agreement of the Authority (both Parties acting reasonably), Service Downtime for Permitted Maintenance which shall take place outside of Operational Hours as defined in Attachment 1- Service Specification of the Order Form

4.2 When the Supplier wishes to carry out any maintenance to the Services (other than Emergency Maintenance) the Supplier will ensure:

a) once agreed with the Authority's Representative the Permitted Maintenance is forthwith entered onto the Maintenance Schedule

b) the Permitted Maintenance is subsequently carried out in accordance with the Maintenance Schedule.

4.3 Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with paragraph 4.1 and 4.2 will be subtracted from the total number of hours in the relevant Service Period when calculating Service Availability, in accordance with paragraph 2 of Part II of Annex 1.

4.4 Service Points shall accrue as set out in paragraph 2 of Part A if any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier (unless the Emergency Maintenance being undertaken is not caused by a Supplier Default), unless otherwise authorised by the Authority.

5 SERVICE CREDITS

5.1 The Authority shall use the Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

PART B: PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within 5 Working Days (or unless otherwise agreed by both Parties of the end of each Service Period, the Supplier shall provide:

(a) a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.2 (the "**Performance Monitoring Report**"); and

(b) a report to the Authority Representative which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.3 (the "**Balanced Scorecard Report**")*.*

Performance Monitoring Report

1.2 The Performance Monitoring Report shall be in such format as stipulated by the Authority and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Performance Indicator and Subsidiary Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous 3 Measurement Periods;

(b) a summary of all Performance Failures that occurred during the Service Period;

(c) the severity level of each KPI Failure which occurred during the Service Period and whether each PI Failure which occurred during the Service Period fell below the PI Service Threshold;

(d) which Performance Failures remain outstanding and progress in resolving them;

(e) for any Material KPI Failures or Material PI Failures occurring during the Service Period, the cause of the relevant KPI Failure or PI Failure and the action being taken to reduce the likelihood of recurrence;

(f) the status of any outstanding Rectification Plan processes, including: (i)

whether or not a Rectification Plan has been agreed; and

(ii) where a Rectification Plan has been agreed, a summary of the Supplier's progress in implementing that Rectification Plan;

(g) for any Repeat Failures, actions taken to resolve the underlying cause and prevent recurrence;

(h) the number of Service Points awarded in respect of each KPI Failure;

(i) the Service Credits to be applied, indicating the KPI Failure(s) to which the Service Credits relate;

(j) Expected Service Uptime achieved per Hosted Service, as required in accordance with Paragraph 17 of Part II of this Annex;

(k) the status of any Contract Change Request or Change Authorisation Note;

(l) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the BCDR Plan;

(m) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

(n) such other details as the Authority may reasonably require from time to time; and

Information in respect of previous Service Periods

(o) a rolling total of the number of Performance Failures that have occurred over the past six Service Periods;

(p) the amount of Service Credits that have been incurred by the Supplier over the past six Service Periods;

Information in respect of the next Quarter

(q) any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter.

Balanced Scorecard Report

1.3 The Balanced Scorecard Report shall be presented in the form of a dashboard as agreed between the Parties from time to time and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period.

1.4 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Board held in accordance with Paragraph 1.5.

1.5 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. The Performance Review Board shall (unless otherwise agreed):

(a) take place within 5 Working Days (unless otherwise agreed by both Parties) of the Performance Monitoring Report being issued by the Supplier;

(b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and be attended by the Supplier Representative and the Authority Representative.

(c) The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure.

2 PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and records (including Supplier's Service Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.

2.3 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

3 PERFORMANCE VERIFICATION

The Authority reserves the right to verify the Availability of the IT Environment and/or the Services and the Supplier's performance under this Agreement against the Performance Indicators including by sending test transactions through the IT Environment or otherwise.

4 SATISFACTION SURVEYS

4.1 In order to assess the level of performance of the Supplier, the Authority may undertake satisfaction surveys in respect of End Users or various groups of End Users (each such survey a "**Satisfaction Survey**"), the results of which may be reflected in the Balanced Scorecard Report. The subject matter of Satisfaction Surveys may include:

(a) the assessment of the Supplier's performance by the End Users against the agreed Key Performance Indicators and Subsidiary Performance Indicators; and/or

(b) other suggestions for improvements to the Services.

ANNEX 1: KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS

PART I: KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS TABLES

The Key Performance Indicators and Subsidiary Performance Indicators that shall apply to the Operational Services are set out below:

1 Key Performance Indicators

1.1 Service Availability

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points
KPI-01	Service Availability	See Paragraph 1 & 2 of Part II of this Annex	Continuous	Above 99.5 % **Target Performance Level:** 99.5% Minor KPI Failure: 99.0% - 99.4% Serious KPI Failure: 98.0% - 98.99% Severe KPI Failure: 97.5% - 97.99%	-2 0 5 10 15 20

1.2 Incident Resolution

No	Key Performance Indicator Title	Definition	Frequency of Measurement	Maximum Resolution Time	Maximum time to respond to a Service Incident	Minimum frequency of updates to the Authority during Service Incident	Severity Levels for Maximum Resolution Time	Service Points

KPI-02	Resolution Time for Severity 1 Service Incidents	See Paragraph 3 of Part II of this Annex	Continuous	2 hours	10 minutes	Every 30 minutes	**Target Performance Level:** Zero Severity 1 Service Incidents not resolved in Maximum Resolution Time Minor KPI Failure: One (1) Severity 1 Service Incident not resolved in Maximum Resolution Time Serious KPI Failure: Two (2) Severity 1 Service Incidents not resolved in Maximum Resolution Time Severe KPI Failure: Three (3) Severity 1 Service Incidents not resolved in Maximum Resolution Time KPI Service Threshold: more than three (3) Severity 1 Service Incidents not resolved in Maximum Resolution Time	0 2 4 6 8

No	Key Performance Indicator Title	Definition	Frequency of Measurement	Maximum Resolution Time	Maximum time to respond to a Service Incident	Minimum frequency of updates to the Authority during Service Incident	Severity Levels for Maximum Resolution Time	Service Points
KPI-03	Resolution Time for Severity 2 Service Incidents	See Paragraph 3 of Part II of this Annex	Continuous	4 hours	30 minutes	Every 2 hours	**Target Performance Level**: Zero Severity 2 Service Incidents not resolved in Maximum Resolution Time Minor KPI Failure: Minor KPI Failure: Two (2) Severity 2 Service Incident not resolved in Maximum Resolution Time Serious KPI Failure: Four (4) Severity 2 Service Incidents not resolved in Maximum Resolution Time Severe KPI Failure: Six (6) Severity 2 Service Incidents not resolved in Maximum Resolution Time KPI Service Threshold: more than six (6) Severity 2 Service Incidents not resolved in Maximum Resolution Time	0 1 3 6 8

KPI-04	Resolution Time for Severity 3 Service Incidents	See Paragraph 3 of Part II of this Annex	Continuous	8 hours	30 minutes	Once per Working Day	Above 95% **Target Performance Level:** 95% Minor KPI Failure: 92.5% - 94.9% Serious KPI Failure: 91.5% - 92.49% Severe KPI Failure: 90.0% - 91.49% KPI	-1 0 1 2 3 4

1.3 Request Fulfilment

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Maximum Completion Time	Time to respond to a Service Request	Minimum frequency of updates to the Authority during Service Request	Service Levels for Maximum Completion Time	Service Points
KPI-05	Completion Time for Service Request (Urgent)	See Paragraph 4 of Part II of this Annex	Continuous	1 Working Day	30 minutes	Once per Working Day	Above 95% **Target Performance Level**: 95% Minor KPI Failure: 92.5% - 94.9% Serious KPI Failure: 91.5% - 92.49% Severe KPI Failure: 90.0% - 91.49% KPI Service Threshold: below 90.0%	-1 0 1 2 3 4

1.4 Subsidiary Performance Indicators

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels
PI-01	% of Supplier's Support Function contacts responded to within 15 minutes	See Paragraph 5 of Part II of this Annex	Continuous	**Target Performance Level:** 99% Service Threshold:
PI-02	% of Severity 1 Service Incidents raised within 10 minutes of reporting	See Paragraph 6 of Part II of this Annex	Continuous	**Target Performance Level:** 99% Service Threshold:
PI-03	% of Severity 2 & 3 Service Incidents raised within 30 minutes of reporting	See Paragraph 7 of Part II of this Annex	Continuous	**Target Performance Level:** 99% Service Threshold:
PI-04	% of Service Requests raised within 30 minutes of receipt	See Paragraph 8 of Part II of this Annex	Continuous	**Target Performance Level:** 99% Service Threshold:
PI-05	% of Major Incident Reports produced within 1 Working Day	See Paragraph 9 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:
PI-06	% of Root Cause Analysis Reports started within 1 Working Day	See Paragraph 10 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:
PI-07	% of Root Cause Analysis Reports for recurring incidents started within 1 Working Day	See Paragraph 11 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:
PI-08	% of Problem Records active more than 10 Working Days	See Paragraph 12 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels
PI-09	% of ITIL Change Requests processed within 5 Working Days	See Paragraph 13 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:
PI-10	% of Operational Change Requests completed in agreed timescales	See Paragraph 14 of Part II of this Annex	Continuous	**Target Performance Level:** 98% Service Threshold:
PI-11	% of updates made to Supplier Asset Register within 5 Working Days	See Paragraph 15 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold**
PI-12	% of updates made to Software Licence Register within 5 Working Days	See Paragraph 16 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold** **Level: 90%**
PI-13	% of updates made to Sub Contracts Register within 5 Working Days	See Paragraph 17of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold** **Level: 90%**
PI-14	% of updates made to Maintenance and Support Agreements Register within 5 Working Days	See Paragraph 18 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold** **Level: 90%**
PI-15	% of updates to Configuration Management System within 5 Working Days	See Paragraph 19 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold** **Level: 90%**
PI-16	% of Severity 4 Service Incidents resolved within Maximum Resolution Time	See Paragraph 21 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold**

PI-17	% of Standard Service Requests completed within Maximum	See Paragraph 22 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold**

No.	Subsidiary Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels
	Completion Time			
PI-18	% of Non-Urgent Service Requests completed within the Maximum Completion Time	See Paragraph 23 of Part II of this Annex	Continuous	**Target Performance Level:** **95% Service Threshold**

PART II: DEFINITIONS AND PERFORMANCE PROCEDURES

1. AVAILABLE

1.1 The IT Environment and/or the Services shall be Available when:

(a) End Users are able to access and utilise all the functions of the Supplier System and/or the Services; and

(b) the Supplier System is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description (as measured on a 24 x 7 basis).

2 SERVICE AVAILABILITY

2.1 Service Availability shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:

$$\text{Service Availability \%} = \frac{(MP - SD)x100}{MP}$$

where:

MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period.

2.2 When calculating Service Availability in accordance with this Paragraph 1:

(a) Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Clause 9.4 (*Maintenance)* shall be subtracted from the total number of hours in the relevant Service Period; and

(b) Service Points shall accrue if:

(i) any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier (unless the Emergency Maintenance being undertaken is not caused by a Supplier Default); or

(ii) where maintenance undertaken by the Supplier exceeds the duration previously agreed with the Authority in any Service Period.

3 INCIDENT RESOLUTION

3.1 When identified by the Authority that the Services have become Unavailable the Authority will report this to the Supplier.

3.2 When identified by the Supplier that the Services have become Unavailable the Supplier must raise a Service Incident and report this to the Authority.

3.3 The start time of a Service Incident will be when reported by the Authority or identified and raised by the Supplier in accordance with the agreed ITSM policy, process and procedure set out the service management obligations / responsibility.

3.4 All Service Incidents must be classified and managed to resolution by the Supplier in accordance with Annex 1, Part 1, Paragraph 1.2 or Paragraph 22 of Part II of this Annex (as applicable).

3.5 The Supplier shall ensure that a Service Incident is resolved within the Maximum Resolution Time.

3.6 Each Service Incident will either be resolved within the Maximum Resolution Time, or it will not; and will be reported as such by the Supplier. The actual incident resolution time is the time taken between the agreed start time and the agreed closure time of the Service Incident (minus any time where activities to resolve a Service Incident has gone beyond a Supplier's Service Boundary).

3.7 Incident Resolution times for Service Incidents shall be measured in Operational Hours.

Worked example: if the Operational Hours for a Service Incident are 0700-2200, then the clock stops measuring Incident Resolution Time at 2200 in the evening and restarts at 0700 the following day.

3.8 In calculating achieved Target Performance as in Paragraph 3.9 and 3.10 below a separate achieved Target Performance Level shall be provided for each severity level.

3.9 For Severity 1 and 2 Service Incidents, achieved Target Performance Level is calculated by determining the number of Service Incidents in the Service Period that have not been resolved within the Maximum Resolution Time.

3.10 For Severity 3 Service Incidents, achieved Target Performance Level is calculated as a percentage of the total number of Service Incidents in a Service Period that should have been resolved within the Target Performance Level using the following formula:

Achieved Target Performance % = (TI-FI) x 100
TI

Where:

TI means the total number of Service Incidents raised during the Service Period; and

FI means the total number of Service Incidents raised during the Service Period that were not resolved within the Target Performance Level.

3.11 During resolution of a Service Incident where the Supplier is dependent on the Authority or the supplier of the Authority for the completion of remedial activities or the provision of information to support its resolution of the Service Incident, this will be deemed as the Service Incident going beyond the Supplier's Service Boundary. Any time whilst the Service Incident is beyond the Service Boundary will be deducted from the total of the actual resolution time.

3.12 At all times during the resolution of a Service Incident the Supplier shall comply with its obligations and responsibilities under the Collaboration Agreement.

3.13 The Service Incident will only be deemed to be Resolved once the Services are Available. However, the Supplier shall not formally close any Service Incident until the Authority has confirmed that the Services are Available.

3.14 The Supplier shall measure Incident Resolution as part of its service management responsibilities and report to the Authority on Incident Resolution as part of the Performance Monitoring Report.

3.15 For the purposes of this Paragraph 3, the following expressions shall have the meanings set opposite them below:

"Operational Hours"	In relation to any Service, the hours for which that Service is to be operational as set out in Schedule 2.1 (*Services Description*);
"Service Incident"	a reported occurrence of a failure to deliver any part of the Services in accordance with the Authority Requirements or the Performance Indicators;

"Severity 1 Service Incident"	a Service Incident which, in the reasonable opinion of the Authority: (a) constitutes a loss of the Service which prevents 50 (fifty) or more End Users from working or impact an entire Authority Site; and /or (b) has a critical impact on the activities of the Authority; and/or (c) causes significant financial loss and/or disruption to the Authority; and/or (d) results in any material loss or corruption of Authority Data;
"Severity 2 Service Incident"	a Service Incident which, in the reasonable opinion of the Authority has the potential to: (a) have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available and/or ; (b) constitute a loss of the Service which prevents between 1 (one) and 50 (fifty) End Users from working or impacts a floor or wing of an Authority Site; and/or (c) cause a financial loss to the Authority which is less severe than the financial loss described in the definition of a Severity 1 Service Failure. •
"Severity 3 Service	a Service Incident which, in the reasonable opinion of the Authority has the potential to have a moderate adverse

Incident"	impact on the activities of the Authority or prevents a single End User from performing their role: •
"Severity 4 Service Incident"	a Service Incident which, in the reasonable opinion of the Authority has the potential to have a minor adverse impact on the provision of the Services to End Users

4 REQUEST FULFILMENT

4.1 The Authority may raise Service Requests. The start time of a Service Request will be when the Supplier receives a request from the Authority in accordance with the agreed ITSM policy, process and procedure set out the service management obligations / responsibility.

4.2 A Service Request must be classified by the Authority and managed to completion by the Supplier in accordance with Annex 1, Part 1, Paragraph 1.3 and Paragraph 23 and 24 of Part II of this Annex.

4.3 The Supplier shall ensure that Service Requests are completed within the Maximum Completion Time.

4.4 Each Service Request will either be completed within the Maximum Completion Time, or it will not; and will be reported as such by the Supplier. The actual completion time for a Service Request is the time taken between the agreed start time and the agreed end time of the Service Request (minus any time where activities to complete the Service Request has gone beyond the Supplier's Service Boundary).

4.5 Service Request completion time shall be measured in Operational Hours.

Worked example: if the Operational Hours for a Service Request are 07:00-22:00, then the clock stops on measuring the Service request completion time at 22:00 in the evening and restarts at 07:00 the following day).

4.6 Achieved Target Performance Level is calculated as a percentage of the total number of the Urgent Service Requests in a Service Period that should have been completed with the Target Performance Level using the following formula:

$$\text{achieved Target Performance (\%)} = \frac{(TSR - FSR) \times 100}{TSR}$$

Where:

TSR means the total number of Urgent Service Requests raised during the Service Period; and

FSR means the total number of Urgent Service Requests raised during the Service Period that were not completed within the Target Performance Level.

4.7 During the delivery time of a Service Request where the Supplier is dependent on the Authority of a supplier of the Authority for the completion of activities or provision of information in support of delivery, this will be deemed as a Service Request going beyond the Supplier's Service Boundary. Any time whilst the Service Request is beyond the Service Boundary will be deducted from the total of the actual delivery time.

4.8 At all times in responding to a Service Request the Supplier shall comply with its obligations and responsibilities under the Collaboration Agreement.

4.9 A Service Request will only be deemed to be completed once the request has been fulfilled. However the Supplier shall not formally close a Service Request until the Authority has confirmed the request is complete.

4.10 The Supplier shall monitor the Service Requests and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

5 SUPPLIER SUPPORT FUNCTION

5.1 The Supplier shall ensure that the Supplier's Support Function contacts are responded to in 15 minutes

(a) Measurement of Supplier's Support Function response times for responding to contacts will be based on when the contact is received by the Supplier's Support Function irrespective of whether it is actioned by a Supplier's Support Operative.

(b) The achieved Target Performance Level is calculated as a percentage of contacts actioned in a Service Period using the following formula:

$$\textbf{achieved Target Performance (\%)} = \frac{\text{Contacts actioned in 15 minutes} \times 100}{\text{Total number of contacts in Service Period}}$$

5.2 The Supplier shall monitor the Supplier's Support Function response times and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

6 PERCENTAGE OF SEVERITY 1 SERVICE INCIDENTS RAISED WITHIN 10 MINUTES OF REPORTING

6.1 For Severity 1 Service Incidents a Supplier shall raise a Service Incident record within 10 minutes of the Service Incident being identified.

6.2 The achieved Target Performance Level is calculated as a percentage of records raised within 10 minutes using the following formula:

$$\textbf{achieved Target Performance (\%)} = \frac{\text{Severity 1 records raised in 10 mins} \times 100}{\text{Total number of Severity 1 Service Incidents in Service Period}}$$

6.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

7 PERCENTAGE OF SERVERITY 2 AND 3 SERVICE INCIDENTS RAISED WITHIN 30 MINUTES OF REPORTING

7.1 For Severity 2 and 3 Service Incidents a Supplier shall raise a Service Incident record within 30 minutes of the Service Incident being identified.

7.2 The achieved Target Performance Level is calculated as a percentage of records raised within 30 minutes using the following formula:

$$\textbf{achieved Target Performance (\%)} = \frac{\text{Severity 2 \& 3 records raised in 30 mins} \times 100}{\text{Total number of Severity 2 \& 3 Service Incidents in Service Period}}$$

7.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

8 PERCENTAGE OF SERVICE REQUESTS RAISED WITHIN 30 MINUTES OF RECEIPT

8.1 A Supplier shall raise a Service Request within 30 minutes of the request being received.

8.2 The achieved Target Performance Level is calculated as a percentage of requests raised within 30 minutes using the following formula:

achieved Target Performance (%) = Service Requests raised in 30 mins x 100
Total number of Service Requests in Service Period

8.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

9 PERECENTAGE OF MAJOR INCIDENT REPORTS PRODUCED WITHIN 1 WORKING DAY

9.1 A Supplier shall produce a Major Incident Report within 1 Working Day of a Severity 1 Service Incident being closed.

9.2 The achieved Target Performance Level is calculated as a percentage of reports produced within 1 Working Day using the following formula:

achieved Target Performance (%) = Major Incident Reports produced within 1 Working Day x 100
Total number of Major Incident Reports produced in Service Period

9.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

10 PERCENTAGE OF ROOT CAUSE ANALYSIS REPORTS STARTED WITHIN 1 WORKING DAY

10.1 A Supplier shall start to produce a Root Cause Analysis Report within 1 Working Day of a Severity 1 Service Incident being resolved.

10.2 The achieved Target Performance Level is calculated as a percentage of reports started within 1 Working Day using the following formula:

achieved Target Performance (%) = Root Cause Analysis Reports started within 1 Working Day x 100
Total number of Root Cause Analysis Reports for Severity 1 Incidents in Service Period

10.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

11 PERCENTAGE OF ROOT CAUSE ANALYSIS REPORTS FOR RECURRING INCIDENTS STARTED WITHIN 1 WORKING DAY

11.1 A Supplier shall start to produce a Root Cause Analysis Report within 1 Working Day of the resolution of a fifth recurring Service Incident that has occurred on the same Configuration Item or End User element of the Services that has been subjected to five (5) Service Incidents (regardless of severity) within any rolling period of six (6) months.

11.2 The achieved Target Performance Level is calculated as a percentage of reports begun within 1 Working Day using the following formula:

$$\textbf{achieved Target Performance (\%)} = \frac{\text{Root Cause Analysis Reports started within 1 Working Day} \times 100}{\text{Total number of Root Cause Analysis Reports for recurring incidents in Service Period}}$$

11.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

12 PERCENTAGE OF PROBLEM RECORDS ACTIVE FOR MORE THAN 10 WORKING DAYS

12.1 A Supplier shall action and close a Problem Record within 10 Working Days of the Problem Record being created by the Supplier.

12.2 The achieved Target Performance Level is calculated as a percentage of the Problem Records closed within 10 Working Days using the following formula:

$$\text{achieved Target Performance (\%)} = \frac{\text{Problem Records closed within 10 Working Day} \times 100}{\text{Total number of Problem Records in Service Period}}$$

12.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

13 PERCENTAGE OF ITIL CHANGE REQUESTS PROCESSED WITHIN 5 WORKING DAYS

13.1 A Supplier shall assess for approval or rejection an ITIL Change Request within five (5) Working Days of the request being submitted.

13.2 The achieved Target Performance Level is calculated as a percentage of requests assessed within 5 Working Days using the following formula:

achieved Target Performance (%) = ITIL Change Request assessed within 5 Working Days x 100
Total number of Change Requests submitted in Service Period

13.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

14 PERCENTAGE OF OPERATIONAL CHANGE REQUESTS COMPLETED WITHIN AGREED TIMESCALES

14.1 A Supplier shall complete a Request for Operational Change (RFOC) within the timescales specified for completion in the RFOC.

14.2 The achieved Target Performance Level is calculated as a percentage of RFOCs completed within agreed timescales using the following formula:

Achieved Target Performance (%) = RFOCs completed within agreed timescales x 100
Total number of RFOCs submitted in Service Period

14.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

15 PERCENTAGE OF UPDATES MADE TO SUPPLIER ASSET REGISTER WITHIN 5 WORKING DAYS

15.1 The Supplier shall reflect all changes (approved by the Authority) made to the Services in the Supplier Asset Register (Schedule 8.5, Paragraph 2.1 (a)). The Supplier shall update the Supplier Asset Register within 5 Working Days of a change being made to the Service.

15.2 The achieved Target Performance Level is calculated as a percentage using the following formula:

Achieved Target Performance (%) = Updates made within 5 Working days of change to a Service x 100
Total number of updates made to Assets Register in Service Period

15.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

16 PERCENTAGE OF UPDATES MADE TO SOFTWARE LICENCE REGISTER WITHIN 5 WORKING DAYS

16.1 The Supplier shall reflect all changes (approved by the Authority) made to the Services in the Software Licence Register (Schedule 8.5, Paragraph 2.1 (a)). The Supplier shall update the Software Licence Register within 5 Working Days of a change being made to the Service.

16.2 The achieved Target Performance Level is calculated as a percentage using the following formula:

$$\textbf{Achieved Target Performance (\%)} = \frac{\text{Updates made within 5 Working days of change to a Service} \times 100}{\text{Total number of updates made to Software Licence Register in Service Period}}$$

16.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

17 PERCENTAGE OF UPDATES MADE TO SUBCONTRACTS REGISTER WITHIN 5 WORKING DAYS

17.1 The Supplier shall reflect all changes (approved by the Authority) made to the Services in the Subcontracts Register (Schedule 8.5, Paragraph 2.1 (a)). The Supplier shall update the Subcontracts Register within 5 Working Days of a change being made to the Service.

17.2 The achieved Target Performance Level is calculated as a percentage using the following formula:

$$\textbf{Achieved Target Performance (\%)} = \frac{\text{Updates made within 5 Working days of change to a Service} \times 100}{\text{Total number of updates made to Subcontracts Register in Service Period}}$$

17.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

18 PERCENTAGE OF UPDATES MADE TO MAINTENANCE & SUPPORT AGREEMENTS REGISTER WITHIN 5 WORKING DAYS

18.1 The Supplier shall reflect all changes (approved by the Authority) made to the Services in the Maintenance and Support Agreements Register (Schedule 8.5, Paragraph 2.1 (a)). The Supplier shall update the Maintenance and Support Agreements Register within 5 Working Days of a change being made to the Service.

18.2 The achieved Target Performance Level is calculated as a percentage using the following formula:

Achieved Target Performance (%) = Updates made within 5 Working days of change to a Service x 100
Total number of updates made to Maintenance & Support Agreements Register in Service Period

18.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

19 PERCENTAGE OF UPDATES MADE TO CONFIGURATION MANAGEMENT SYSTEM WITHIN 5 WORKING DAYS

19.1 The Supplier shall reflect all changes (approved by the Authority) made to the Services in the Configuration Management System (Schedule 8.5, Paragraph 2.1 (b)). The Supplier shall update the Configuration Management System within 5 Working Days of a change being made to the Service.

19.2 The achieved Target Performance Level is calculated as a percentage using the following formula:

Achieved Target Performance (%) = Updates made within 5 Working days of change to a Service x 100
Total number of updates made to Configuration Management System in Service Period

19.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

Crown Commercial Service

20 EXPECTED SERVICE UPTIME

20.1 The Supplier shall report as part of the Performance Monitoring Reports, on the Expected Service Uptime of the Services within each Service Period

21 PERCENTAGE OF SEVERITY 4 SERVICE INCIDENTS RESOLVED WITHIN MAXIMUM RESOLUTION TIME

21.1 A Supplier shall resolve a Severity 4 Service Incident within 5 Working Days.

21.2 The achieved Target Performance Level is calculated as a percentage of Severity 4 Service Incidents resolved within 5 Working Days using the following formula:

Achieved Target Performance (%) =
Severity 4 Service Incidents resolved within 5 Working Days x 100
Total number of Severity 4 Service Incidents raised in Service Period

21.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

22 PERCENTAGE OF STANDARD SERVICE REQUESTS COMPLETED WITHIN MAXIMUM COMPLETION TIME

22.1 A Supplier shall complete a Standard Service Requests within 3 Working Days.

22.2 The achieved Target Performance Level is calculated as a percentage of Standard Service Requests completed within 3 Working Days using the following formula:

Achieved Target Performance (%) =
Standard Service Requests completed within 3 Working Days x 100
Total number of Standard Service Requests raised in Service Period

22.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

23 PERCENTAGE OF NON-URGENT SERVICE REQUESTS COMPLETED WITHIN MAXIMUM COMPLETION TIME

23.1 A Supplier shall complete Non-Urgent Service Requests within 5 Working Days.

23.2 The achieved Target Performance Level is calculated as a percentage of Non-Urgent Service Requests completed within 5 Working Days using the following formula:

Achieved Target Performance (%) = Non-Urgent Service Requests completed within 5 Working Days x 100
Total number of Non-Urgent Service Requests raised in Service Period

23.3 The Supplier shall monitor this Subsidiary Performance Indicator and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

2.6.1 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
[redacted]	Account Manager	Contract Period
[redacted]	Service Manager	Contract Period

Part B – Key Sub-Contractors

Not Applicable

Crown Commercial Service

Attachment 6 – Software

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

2.6.2 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

Not Applicable

Part B – Third Party Software

The Third-Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry
[redacted]	[redacted]	Backup	270TB, further licenses available if needed	None	1	COTS	Annual
[redacted]	[redacted]	Backup	270TB, further licenses available if needed	None	1	COTS	Annual
[redacted]	[redacted]	Vulnerability Management	1	None	1	COTS	Annual
[redacted]	[redacted]	Network Monitoring	1	None	1	COTS	Annual

[redacted]	[redacted]	Service Management	Sufficient for Agilisys team members	None	1	COTS	Annual

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	Dun and Bradstreet Overall Business Risk	Low-Moderate
Guarantor	N/A	N/A

PART B – RATING AGENCIES

Not Used

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE
Not Used

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 Programme Board	Service Management Lead Service Management team lead Infrastructure team leads Business Operations team leads
Supplier members of Programme Board	Account Manager Service Manager
Start Date	Within 1 month of service transition being completed.
Frequency	Monthly Meetings
Location	In person meetings to be held in Stella House or remotely via Teams

Operational Board	
Buyer Members of Operational Board	Head of Cyber Security & Infrastructure services Head of Governance Service Management Leads Infrastructure Services team Leads Finance Lead Commercial Lead Business operations Lead
Supplier Members of Operational Board	Account Manager Service manager

Start Date	Within 1 month of service transition being completed.
Frequency	Monthly
Location	In person meetings to be held in Stella House or remotely via Teams

Strategic Management Board	
Buyer Members for Strategic Management Board	Chief Digital, Data and Technology Officer Heads of Service Commercial Lead
Supplier Members for Strategic Management Board	Account Manager
Start Date	Within 1 month of contract award
Frequency	Quarterly
Location	In person meetings to be held in Stella House or remotely via Teams

- Exit Board to be constituted during the life of the contract.

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

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: Chris Gooday, Information Governance Manager - dataprotection@nhsbsa.nhs.uk

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **supplierdataprotection@agilisys.co.uk**

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

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • NHSBSA data stored within the CHDC. The Supplier will have access to all NHSBSA data stored with CHDC for the purposes of the provision of a backup and restore service. • The Supplier are also responsible for managing the hardware infrastructure that hosts NHSBSA data; however, this will not involve the processing of personal data as it is in relation to hardware only. 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 contract 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.
Duration of the processing	For the duration of this Contract.
Nature and purposes of the processing	The nature and purposes processing are for the provision of a backup and restore service to NHSBSA for data stored within the CHDC.
Type of Personal Data	The Supplier will process both personal data and special category data processed across all NHSBSA business areas, for the purposes of the provision of backup and restore of NHSBSA data within the CHDC.
Categories of Data Subject	The categories of data subject across all NHSBSA business areas whereby data is stored within the CHDC, including, but are not limited to: • Staff (including volunteers, agents and temporary workers) • Customers and clients • Suppliers • Patients • Students and pupils • Members of the public

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	The Supplier will retain NHSBSA data in line with NHSBSA retention periods. In the event the contract is terminated, the Supplier will return NHSBSA data via a secure mechanism as instructed by NHSBSA.

Attachment 10 – Transparency Reports

The following will be reported as part of Project Santiago- Cabinet Office Reporting on a quarterly basis.

KPI Description	Good Target	Approaching Target Threshold	Requires Improvement Threshold	Inadequate Threshold
Service Availability of Infrastructure that support Business Services	99.5%	98%	97.5%	97.49%
Resolution Time for Severity 1 Service Incidents (Maximum Resolution Time = 2 hours)	Zero Severity 1 Service Incidents not resolved in Maximum Resolution Time	Two Severity 1 Service Incidents not resolved in Maximum Resolution Time	Three Severity 1 Service Incidents not resolved in Maximum Resolution Time	More than three Severity 1 Service Incidents not resolved in Maximum Resolution Time
Resolution Time for Severity 2 Service Incidents (Maximum Resolution Time = 4 hours)	Zero Severity 2 Service Incidents not resolved in Maximum Resolution Time	Four Severity 2 Service Incidents not resolved in Maximum Resolution Time	Six Severity 2 Service Incidents not resolved in Maximum Resolution Time	More than six Severity 2 Service Incidents not resolved in Maximum Resolution Time

Social Value KPI Reporting				
Theme(s) Selected	**Overall Target Commitment(s)**	**Commitment Activities**	**Regularity of Reporting**	**Reporting Metric(s)**
Fighting Climate Change	Reporting of emissions footprint for Agilisys Service Delivery on the contract	Scope 3 reporting for Categories 5 – Waste generated in operations & 6 – Business Travel	Annual reporting	Emissions associated with delivering the services in CO2 equivalent (CO2e) kg / tonne
Fighting Climate Change	Reporting of NHSBSA Crown Hosting located infrastructure emissions	Scope 2 emissions reporting on grid electricity in Crown Hosting (subject to Authority providing authority to engage with Crown Hosting	Annual reporting	Emissions associated with the grid electricity and standby power in Crown Hosting in CO2 equivalent (CO2e) kg / tonne
Fighting Climate Change	Establish comprehensive emissions baseline for all Agilisys scope 1, 2 & 3 emissions in 2025	Ensure our reporting accurately reflects the full extent. of our emissions footprint across all our business units beyond minimum compliance.	Annual reporting	Annual report on the Agilisys Carbon Reduction Plan
Tackling Workplace Inequality	Zero employees on this contract without evidence of compliance with employment law.	Payroll may not release remuneration until employment check is completed.	Reported by exception.	Absolute number of hires with incomplete employment checks.
Tackling Workplace Inequality	Reduced gender pay gap	Diversity objectives for leadership • Inclusive hiring	Annual reporting	• Gaps between measures of

		• Diversity networks which support individual's professional success. • Learning, Education and Development on diversity and inclusion. • Reward Strategy improvements		mean pay and median pay for men and women. • Proportion of men and women receiving a bonus. • Gaps between measures of mean bonus pay and median bonus pay for men and women. • Gender splits by pay quartile.

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

https://assets.crowncommercial.gov.uk/wp-content/uploads/RM6100-Lots-2-3-and-5-Call-Off-Terms-v3.docx

https://assets.crowncommercial.gov.uk/wp-content/uploads/RM6100-Lots-2-3-and-5-Additional-and-Alternative-Terms-and-Conditions-v2.00.odt

Agreed changes and clarifications to the Call Off Terms and other provisions of the Contract.

1. Clause 19.4.2 replace £10million with "150% of the Charges paid and/or due to be paid to the Supplier under this Contract in the Contract Year immediately preceding the occurrence of the Default;"

2. 19.4.3 delete "and Compensation for Critical Service Level Failure"

3. 19.5 Not used

4. Schedule 2 Part C section 3.1 replace "this Paragraph" with "the Order Form"

5. Schedule 2 Part C section 3.2.1 delete

6. Schedule 2 Part C section 3.2.2 delete "on 31 January"

7. 'Buyer Responsibilities' include the selection and licensing of the Third Party COTS Software applications except for those identified as 'Supplier responsible'. The Supplier's responsibilities in relation to such software shall be limited to managing the implementation and performance of the software and liaising with the suppliers in relation to fixing any performance issues. The Buyer shall be responsible for enforcing the terms of any licensing and support arrangements with the suppliers and securing any remedies for unsatisfactory performance. Clause 27 shall not apply to IPR Claims related to software in this category.

8. The Supplier's responsibilities in relation to the Third-Party COTS Licensed Software applications identified as 'Supplier responsible' include the licensing of the software, managing the implementation and performance of the software and liaising with the suppliers in relation to fixing any performance issues. For software within this category, the Buyer will be bound by the licensing and support terms of the third-party supplier in question including in relation to IPR Claims. The Supplier shall be responsible for taking reasonable steps to enforce the terms of any licensing and support arrangements with the suppliers and securing any available remedies for unsatisfactory performance. The remedies received from the suppliers shall be the Supplier's exclusive liability to the Buyer for unsatisfactory performance of the software.

9. 'Buyer Responsibilities' include the selection and procurement of all aspects of the Buyer System, Buyer Software, Buyer Assets and Operating Environment except those elements expressly identified as 'Supplier responsible'. The Supplier's responsibilities in relation to such elements shall be limited to managing the implementation and performance of such elements and liaising with the suppliers in relation to fixing any performance issues. The Buyer shall be responsible for enforcing the terms of any licensing and support arrangements with the suppliers and securing any remedies for unsatisfactory performance. Clause 27 shall not apply to IPR Claims related to items in this category.

10. Where the Supplier validly refers off identified performance issues to third party suppliers, this will 'stop the clock' in terms of the Supplier's performance against the Service Levels / Services Specification until such time as the supplier provides a resolution back to the Supplier for implementation.

11. During the Term, the Supplier may reasonably identify that any aspect of the Buyer Systems, Buyer Software, Buyer Assets and Operating Environment needs replacing, upgrading or supplementing. If the Buyer declines to follow such recommendation, the Supplier shall not be responsible for any performance issues that arise as a result and shall be entitled to render reasonable additional charges to reflect any additional work caused as a result.

12. Clauses 26.9 / Clause 27/ Clause 34/ S3 & S6. The Supplier's obligations under these clauses and Schedules shall be subject to the agreed scope of the Services. Any liability of the Supplier under Clause 27.3 shall be subject to the Supplier being in Default.

13. Clause 34 The Buyer is responsible for establishing the adequacy of the Protective Measures, the Security Management Plan, ISMS, Baseline Security Requirements and the Buyer Security Policy.

14. It is acknowledged that the Supplier's BCDR Plan shall relate to the Services not the Buyer Systems, Buyer Software, Buyer Assets and Operating Environment themselves.