58. Hosting of Applications

58.1 Hosting of Applications

Ref	Level	Owner	Description
58.1.1	L3	Supplier	The Supplier shall manage a cloud-hosting capability for Authority Services, where required, in accordance with the Authority's Technical Framework Document.
58.1.2	L3	Supplier	The Supplier shall maintain any hosted resources in accordance with the cloud vendor's support and security guidance.
58.1.3	L3	Supplier	The Supplier shall operate any cloud-hosting environments in accordance with the Authority's Information Security Policy and Standards and in accordance with the Technical Framework Document.
58.1.4	L3	Supplier	The Supplier shall support and manage the cloud hosting of in-scope services, cost effectively, within their scope, including but not limited to areas such as auto-provision and auto-scaling.
58.1.5	L3	Supplier	The Supplier shall manage the cloud hosting platforms using the Authority's cloud management platform tools.
58.1.6	L3	Supplier	The Supplier shall deliver a managed orchestration capability for their Services, within the Supplier and with other third party providers where appropriate.
58.1.7	L3	Supplier	The Supplier shall provide scheduling and implementation of required Updates and patches to the hosting environment, co-ordinating as appropriate with the Authority, and to minimise impact to the availability of the Services.
58.1.8	L3	Supplier	The Supplier shall be responsible for the maintenance, and creation of new where required, hosting resource configuration and Policies, in accordance with the Authority's Policies, Processes and Standards as applicable, e.g. Role Based Access Control (RBAC).
58.1.9	L3	Supplier	The Supplier shall manage the hosting audit log in accordance with the Authority's Policies for data retention.
58.1.10	L3	Supplier	The Supplier shall provide configuration and support of the cloud hosting backup service in accordance with the Authority's Production Control Procedures.
58.1.11	L3	Supplier	The Supplier shall provide the capability to undertake ad-hoc backups of the cloud hosting services and agree the Process for the provision of this activity with the Authority.
58.1.12	L3	Supplier	The Supplier shall carry out regular checks on the success of backups, and perform Test restores to ensure the data is recoverable when required.
58.1.13	L3	Supplier	The Supplier shall ensure that an automated failover capability is configured for the cloud hosting services where agreed with the Authority and in accordance with the Authority's Change Management Policies and Processes.
58.1.14	L3	Supplier	The Supplier shall be responsible for the identity management of End User Accounts and role-based access for cloud hosting services within their scope.
58.1.15	L3	Supplier	The Supplier shall provide configuration, maintenance and support of the infrastructure as code in accordance with the Authority's Production Control Procedures.
58.1.16	L3	Supplier	The Supplier shall undertake infrastructure as code management to ensure the configuration is maintained as the service evolves over time as part of managed change to the Service.
58.1.17	L3	Supplier	The Supplier shall provide configuration and maintain the monitoring capability of the cloud hosting services within their scope, in accordance with the Authority's Production Control Procedures.

58.1.18	L3	Supplier	The Supplier shall provide ongoing improvements and enhancements to the monitoring services for cloud hosting as agreed with the Authority.
58.1.19	L3	Supplier	The Supplier shall provide regular information to the Authority against the consumption of cloud hosting services and provide trend analysis against capacity planning.
58.1.20	L3	Supplier	The Supplier shall provide validation of and information against the Charges incurred for cloud hosting services and ensure that analytics and recommendations are provided to improve the future consumption and cost reduction of services within their scope.

58.2 Gated Governance

Ref	Level	Owner	Description
58.2.1	L3	Supplier	The Supplier shall support the preparation of information related to the provision of Services and required by the Authority for the Gated Review Process and in alignment with the Office of Government Commerce's Projects In Controlled Environments (PRINCE2), Managing Successful Programmes (MSP) or any agile methodology as required by the Authority, and in accordance with Schedule 2.3 (*Standards*).

58.3 Implementation Planning

Ref	Level	Owner	Description
58.3.1	L3	Supplier	The Supplier shall agree with the Authority the implementation plan for each new or changed application or New Release.
58.3.2	L3	Supplier	The Supplier shall comply with its obligations pursuant to each agreed implementation plan.

58.4 Transition Management – Per Release

Ref	Level	Owner	Description
58.4.1	L3	Supplier	The Supplier shall engage in and support the transition management process.

58.5 Pilot Testing

Ref	Level	Owner	Description
58.5.1	L3	Supplier	The Supplier shall produce, maintain and provide to the Authority pilot Test Plans where required.
58.5.2	L3	Supplier	The Supplier shall participate in the execution of pilot Testing including re-Testing and regression Testing as necessary, in accordance with Schedule 6.2 (Testing Procedures)..

Future Services

59. Future Services

59.1 General

59.1.1 The Supplier acknowledges that nothing in this Paragraph 59 shall oblige the Authority to take any Future Services from the Supplier or prevent the Authority from receiving services or projects similar or identical to the Future Services from any third party.

59.1.2 The Supplier shall, at all times during the Term:

(a) provide all Future Services requested by the Authority in accordance with this Agreement (provided that such request complies with this Paragraph 59); and

(b) ensure that it is able to provide Future Services as requested by the Authority in accordance with this Paragraph 59 without any risks or impacts (including any arising in connection with the Implementation, Testing or operational use of such or Future Services) to:

a. the rights and obligations of either Party under this Agreement; and

b. to the provision of Goods and Services by the Supplier to the Authority in accordance with this Agreement
(each a "**Risk/Impact**").

59.1.3 The Supplier shall ensure that, at all times during the Term, the Future Services comply with all requirements applicable to the Goods and Services (including as set out elsewhere in this Agreement).

59.2 Calling-off Future Services

59.2.1 The Authority may notify the Supplier that it requires any Future Service by issuing a Contract Change Request to the Supplier in accordance with the Change Control Procedure.

59.2.2 Subject to Paragraph 59.2.4 of below, the Parties shall follow the Change Control Procedure to agree the provision of the Future Service, which shall include documenting, in respect of the relevant Future Service:

(a) any additional or variant terms and conditions;

(b) the Authority Requirements;

(c) Milestones and an Implementation Plan (in accordance with Schedule 6.1 (*Implementation Plan*));

(d) the Testing procedures (in accordance with Schedule 6.2 (*Testing Procedures*));

(e) any additional Charges (in accordance with Schedule 7.1 (*Charges and Invoicing*));

(f) performance levels (in accordance with Schedule 2.2 (*Performance Levels*));

(g) any applicable Change to this Schedule;

(h) any applicable Change to Schedule 8.5 (*Exit Management*); and

(i) any applicable Change to Schedule 11 (*Processing of Personal Data*).

59.2.3 In addition to the obligations set out in Schedule 8.2 (*Change Control Procedure*), the Supplier shall, as part of the Impact Assessment provided by the Supplier in relation to such Contract Change Request:

(a) without prejudice to Paragraph 59.1.2 above, inform the Authority of every Risk/Impact (and potential Risk/Impact) and how it proposes to mitigate or remove such Risk/Impact; and

(b) promptly provide all information and assistance necessary to enable the Authority to assess the nature, risk or impact of any Risk/Impact (or potential Risk/Impact) or any proposal made by the Supplier under Paragraph 59.2.3(a) above.

59.2.4 Notwithstanding any provisions of Schedule 8.2 (*Change Control Procedure*), the Supplier acknowledges and agrees that if a Future Service is called-off by the Authority in accordance with this Paragraph 59.2, any failure by the Supplier to implement, Test and commence the provision of a Future Service shall be a Default by the Supplier.

59.2.5 The Supplier shall, at no additional cost to the Authority, implement and commence provision of any other services, functions and responsibilities which are either necessary for, or incidental to, the proper performance by the Supplier of the Future Service.

59.2.6 The Future Services are set out in Paragraphs 59.3 to 59.5 below.

59.3 Home Printing Requirements

Ref	Level	Owner	Description
59.3.1	L3	Supplier	The Authority has future plans for the introduction of home printing requirements. These are articulated in the Authority's Technical Framework Document. If the Authority decides to introduce these services, the Authority shall do so in accordance with the provisions of this Paragraph 59.

59.4 VDI Requirements

Ref	Level	Owner	Description
59.4.1	L3	Supplier	The Authority has future plans for the introduction of VDI requirements. These are articulated in the Authority's Technical Framework Document. If the Authority decides to introduce these services, the Authority shall do so in accordance with the provisions of this Paragraph 59.

59.5 BYOD Requirements

Ref	Level	Owner	Description
59.5.1	L3	Supplier	The Authority has future plans for extending the existing BYOD service in terms of scope and scale. These are articulated in the Authority's Technical Framework Document. If the Authority decides to introduce these services, the Authority shall do so in accordance with the provisions of this Paragraph 59.

60. Glossary

The following terms used in this Schedule shall have the following meaning:

Definition	
Access Management	means the execution of Authority's Policies and actions defined in information security and Availability Management, as well as the process of granting Authorised End Users right to use a service and helps to protect the confidentiality, integrity and availability of assets and information;
Access Profiles	means the collection of settings and information associated with an End User;
Access Point	means a base station or network access point in a WLAN network, consisting of a radio (often more than one) and a network connection, enabling WLAN clients to access network resources connected to an enterprise network;
Accessibility Assessment	means the assessment that takes place to understand the Authority's accessibility requirements;
Accessibility Demonstration	means the demonstration of one or more related pieces of IT Peripheral Equipment and/or Accessibility Software either as part of or following an Accessibility Assessment to a prospective Enhanced Accessibility Service End User, Standard Accessibility Service End User or as otherwise requested by the Authority;
Accessibility End User	means the Authority's End User that is a recipient of the Accessibility Solutions;
Accessibility Software	means a set of software and related services that enable physically impaired members of the Authority's organisation to access and make full use of IT services;
Accessibility Solution	means a set of hardware, software and related services that enable physically impaired members of the Authority's organisation to access and make full use of IT services;
Alert	means the automatic notification received from a Software monitoring tool indicating a potential Incident;
Application Access Control Lists	means a list of permissions attached to an object as specified in the Authority security document;
Architecture Management	means the management practice that establishes, maintains and uses a coherent set of guidelines, architecture principles and governance regimes that provide direction and practical help in the design and development of an enterprise's architecture to achieve its vision and strategy;
Architecture Standards	means those standards relating to the overall design of a computing system and the logical and physical inter-relationships between its components;
Asset and Configuration Management	means a process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed;
Asset Management Database	means the database maintained by the Supplier which contains asset information relating to the provision of the Services;
Authentication Services	means services that enable organisations to keep their networks secure by permitting only authenticated End Users (or processes) to access its protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services;
Authorised End Users	means any individual End User within the Authority, Authority Group or any Service Recipient who is authorised by the Authority to use or receive a specific service;
Authority Personnel	means any individual End User working for the Authority;

Authority Services	means the totality of all services being provided to the Authority by: (i) the Supplier; (ii) the Authority; and (iii) Other Suppliers;
Availability	means the same as Service Availability;
Availability Management	means the process of defining, agreeing, documenting and managing Availability;
Availability Plan	means a plan that ensures that existing and future Availability Requirements for IT Services can be provided using effective cost measures;
Change Management	means the management for all Changes to any environment and provides a standard, consistent and robust method of delivering authorised change.
Configuration Items (CI)	means a unit of infrastructure which is under Configuration Management and appears in the CMDB (refers to the fundamental structural unit of a Configuration Management system (examples of CIs include individual requirements documents, software, models, and plans);
Configuration Management	means a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life;
Configuration Management Database (CMDB)	means the database containing all the entities and attributes that describe the hardware and software assets used by the Authority to deliver Services;
Continual Service Improvement	means the process of continually aligning and re-aligning IT services to the changing business needs by identifying and implementing improvements to IT services that support business processes;
Definitive Media Library	means one or more locations in which the definitive and approved versions of all media Configuration Items are securely stored;
Directory Services	means a customisable information store that functions as a single point from which End Users can locate resources and services distributed throughout the network. This customisable information store also gives administrators a single point for managing its objects and their attributes;
Emergency Operational Change	means an Operational Change that must be introduced as soon as possible – for example, to resolve a Major Incident or implement a security patch;
Enhanced VIP Services (E-VIP Services)	means those Services being delivered to E-VIP End Users in accordance with the Target Performance Levels and Performance Indicators in Schedule 2.2 (*Performance Levels*);
End-Point Control	means a policy-based approach to network security that requires End User Client Devices to comply with specific criteria before they are granted access to network resources;
End-Point Encryption	means the encryption of End User Client Devices connected to the network;
End User Account	means the electronic system record that provides, to a single End User, appropriate access to IT Services;
End User Client Device	means any client computing, laptop, tablet, removable storage media or mobile device;
Escalation Matrix	means a document that specifies multiple stakeholders to be notified in the event of critical issues;
Event Management	means the process that monitors all events that occur through the IT infrastructure and allows for the detection and escalation of exception conditions to those expected for normal operation;
Event(s)	means a change of state that has significance for the management of an IT service or other Configuration Item (CI);
External Gateway Services	means the facility whereby the Supplier provides for the secure connection of third party sites to the Authority's application services;
Facilities Management Contractor (FMC)	means the Authority's contractors responsible for managing the Authority's facilities

Firewall	means a set of related programs, located at a network gateway server, designed to protect the resources of the Authority's network from users of another network;
Gated Review Process	means the Authority approval process for acceptance of Project Deliverables;
Gateway	means an intermediate device that connects two (or more) computer networks that that is out of bounds for the host network nodes, serves as the entry and exit point on a network and enables either one-way or two-way communication between the connected networks;
Gateway Services	means the facility whereby the Supplier provides for the secure connection of the Authority's application services;
Government Security Classification Scheme	means the Government's Security Classification Scheme; a policy describing how HM Government classifies information assets to: ensure they are appropriately protected; support UK Public Sector Business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners;
Health and Social Care Network (HSCN)	means a new data network for health and care organisations which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently;
Identity and Access Management Service	means the framework of business processes, technologies, Policies and Procedures used to create trusted digital identity representations of individuals and non-person entities, bind those identities to credentials that may serve as a proxy for the individual or non-person entities in access transactions, and leverage the credentials to provide authorised access to Authority's resources;
IMACDs	means installation, move, add, change, and disposal;
Inactive Port(s)	means those Active Ports which, notwithstanding the recording of that port as being activated by the Supplier for use by the Authority, have not been used during the previous Service Period;
Incident	means an unplanned interruption to an IT service, or a reduction in the quality of an IT service, or a failure of a Configuration Item that has not yet impacted an IT service;
Incident Management	the process that handles all failures, faults or questions in order to restore a Service to the Authority as soon as possible or to respond to Service Requests;
Incident Models	means the models that contain the pre-defined steps that should be taken for dealing with a particular type of Incident. This is a way to ensure that routinely occurring Incidents are handled efficiently and effectively;
Information Security Event	means a notification typically created by an IT service, configuration item or monitoring tool – relating specifically to security services and any occurrence related to assets or the environment indicating a possible compromise of Policies or failure of controls, or an unmapped situation that can impact security;
Information Security Incident	means one or more information security events that compromise business operations and information security;
Inter-Domain Gateway	An Inter-Domain Gateway is used to demarcate the boundary of two or more IT Environments that have different risk profiles or Accreditation scopes and manage Information Assets at different Impact Levels or Protective Marking. An Inter-Domain Gateway is used to implement security controls to protect Information Assets held within and transferred between such IT Environments. Typically, these may include controls such as an accredited protocol break to restrict communications to specific authorised protocol flows and content across the boundary. An Inter-Domain Gateway may be used to connect the Supplier's IT Environment to public networks and to those provided by Other Suppliers who may or may not be connected to the PSN;

IT Service Continuity Management (ITSCM) Event Closure Report	means a report produced by the Service Integration Supplier following the closure of an ITSCM Test Event;
IT Service Continuity Management (ITSCM) Policies and Process	means the documented Authority Policies and Processes relating to ITSCM that shall be followed by the Supplier;
IT Service Continuity Management (ITSCM) Procedures	means the associated Procedures relating to ITSCM that have been defined to support the Policies and Processes;
IT Service Continuity Management (ITSCM) Strategy	means the document recording the strategy for ITSCM that shall be provided by the Supplier;
ITSCM Event	means an Event related to IT Service Continuity;
ITSCM Test Event	means a simulation of an ITSCM Event executed in accordance with the ITSCM Test Programme and the ITSCM Policies and Procedures;
ITSCM Test Programme	means a programme for the conduct of ITSCM Test Events;
IT Systems	means a computer system or set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself;
IT Infrastructure Library (ITIL)	means a defined series of best practice and processes for IT service management (ITSM) that focuses on aligning IT services with the needs of business;
ITSM Product	means the IT service management (ITSM) tool provided by the Supplier, that provides as a minimum workflow functionality and tools for optimally developing, delivering, and managing IT services. ITSM is used to handle Incidents, Service Requests, Problems, and Changes;
Service Knowledge Management	provision of and access to appropriate level of knowledge and information artefact relating to the provision, support and transition of services;
Known Error Database (KEDB)	means a database that describes all of the known issues within the overall systems and describes the situations in which these issues appear, and when possible, it offers a workaround that will get the End User around the problem and back to productive work;
Known Error Records	means a record that has a documented root cause and a workaround;
Known Errors	means a Problem that has a documented root cause and a workaround;
Knowledge Base	means a logical database containing data and information used by the Service Knowledge Management System;
LAN Port	means the LAN switch port (including all LAN equipment and interconnecting infrastructure at a Site other than floor distribution cabling) providing Authority equipment connectivity;
Lessons Learnt	means a list of documented observations and actions arising from the root cause analysis of an Incident or Problem or other Service-related issues;
Local Area Network (LAN)	means a computer network that links devices within a building or group of adjacent buildings,
Major Incident	means a Severity 1 Incident or Severity 2 Incident;
Master Time Reference	means the source of time agreed between the Parties that ensures all time values are consistent to within an agreed tolerance;

N-1	means in relation to software, the immediately preceding major release of that software (but excluding for the avoidance of doubt interim releases, fixes and patches);
Network Availability	means the availability of a service provider's IP network;
Network Printer(s)	means a printer connected to the Network which is either: (i) purchased from the Products and Services Catalogue; or (ii)in existence at the CCN Effective Date;
New Applications	means an application or a suite of applications that are proposed to be, or, have been transitioned into live services and have been taken into support;
Non-Production Environment	means all IT environments other than the Production Environment;
Normal Service	means the performance of a Service fully in accordance and compliance with the Services Descriptions in this Schedule and the Performance Indicators and Target Performance Levels in Schedule 2.2 (*Performance Levels*);
Normal Service Restoration Plan	means a plan to restore Normal Service following the declaration of an ITSCM Event;
Operating Procedures	means the detailed description of the activities and tasks necessary to deliver the Services, produced by the Supplier in accordance with the Authority's Policies and Processes
Operational Change Request	means the same as Request for Change;
Operational Level Agreement (OLA)	means an agreement that describes the responsibilities of internal support groups toward other support groups;
Other Tooling	means all tooling other than the ITSM Product that the Supplier will be delivering to the Authority as part of the Suppliers obligations to deliver the Services;
Password Management Policy	means a set of rules designed to enhance computer security by encouraging End Users to employ strong passwords and use them properly;
Peripheral Equipment	means an ancillary device used to connect to computers;
Presence and Instant Messaging Service	means a type of service that enables End Users to observe the presence status of other authenticated End Users (online, offline, busy, or away) and provides instant access to interaction options, such as instant messages (IM), mail, and phone conferences;
Print Device	means any physical device (including bios and firmware) that is connected to a local device or a print server and prints paper documents;
Priority Matrix	a priority matrix defines, in advance, internal priorities for Service Tickets that specify given combinations of impact and urgency;
Problem Management	means the process for managing the lifecycles of all Problems;
Problem Record(s)	means a Record of a Problem in the Supplier's ITSM Product;
Product Catalogue	means a document that provides information about specific versions or configurations of an asset;
Production Control	means the activity of monitoring and controlling a large physical facility or physically dispersed service, including a set of actions and decision taken during production to regulate output and obtain reasonable assurance that the specification will be met.
Production Control Procedures	means the library of information and Procedures managed by the Supplier and used to guide the Supplier and the Authority in the day to day delivery and receipt of the Services;
Production Environment(s)	means the same as Live Environment;
Products and Services Catalogue	means an organised and curated collection of any and all business and information technology related services that can be performed by, for, or within an enterprise;

Public Key Infrastructure	means the set of roles, Policies, and Procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption;
Public Services Network (PSN)	means the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources;
Quality of Service (QOS)	means a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity;
Removable Storage Media	means any type of storage media that can be removed from a computer while the system is running;
Request for Change (RFC)	means a formal proposal for an alteration to some any Service delivered by the Supplier in accordance with the Authority's Change Management Policies and Processes;
Request Fulfilment	means the fulfilment of a Service Request from an End User for information, advice, a Standard Change, or access to a service;
Request Fulfilment Tool	means the ITSM Product used by both the Authority and other service providers to manage the fulfilment of Service Requests;
Responsibility Matrices	means the obligations of the Supplier in respect of their services and the responsibilities of the Authority (if any) in respect of each such obligation;
Role Based Access Control (RBAC)	means an approach to restricting access to End Users to the Authority's IT Environment;
Security Accreditation	means the accreditation by the Authority of the Supplier's compliance with the Information Security Policies and Standards;
Security Impact and Risk Report	means the report provided by the Supplier to the Authority and its agents regarding any proposed amendments to the Information Security Policies and Standards affecting the Services;
Security Operations Centre (SOC) Supplier	means the entity from time to time providing the SOC security management services to the Authority, which at the Effective Date is the Supplier;
Security Risk	means the probability of exposure or loss arising from a cyber-attack or data breach resulting in the potential loss or harm related to technical infrastructure, use of technology or reputation of the Authority;
Self-Service Facilities	means electronic support that allows End Users to access information and perform routine tasks relating to IT service management activities without needing the help of a live service desk representative;
Service Demand Management	means the process that helps a business understand and predict Authority demand for services; this includes all forms of demand from the business for people, services and their associated assets;
Service Desk Supplier	means the entity from time to time providing the Service Desk Services to the Authority, which at the Effective Date is the Supplier;
Service Improvement Plans (SIPs)	means a formal plan that has been produced in accordance with the Continual Service Improvement Management Policies and Processes to implement improvements to a Service;
Service Level Management	ensures that the agreed level of service is provided for all Services and that all future services are delivered to agreed achievable targets;
Service Management	means all activities undertaken by the Supplier to manage the Services;
Service Management Tool(s)	means the ITSM Software that supports the Service Management function;
Service Portfolio Management	means the process responsible for the assembly of an initial 'service design package' (SDP) for each service and its maintenance through the Service life cycle;
Service Requests	has the meaning given to it in Schedule 2.2 (*Performance Levels*);

Service Restoration	means the action(s) taken to return an IT service to the End Users after repair and recovery from an Incident;
Service Reviews	means a review of the Service(s) being delivered by a Supplier, conducted in accordance with the Service Level Management Policies and Processes;
Service Suppliers	means the third parties who have contracted directly with the Authority to provide services;
Service Validation and Testing	means the process of planning and implementing a structured validation and test process that provides objective evidence that the new or changed service will support the Authority's business and stakeholder requirements, including the agreed Performance Indicators and Target Performance Levels;
Single Sign On (SSO)	means an authentication process that allows a End User to access multiple applications with one set of login credentials;
Standard Accessibility Service End User	means an individual who requires slight adaptations to be made to their Accessibility Solution in order that they can access and make full use of IT services;
Standard Change	means a change to a Service or infrastructure for which the approach is pre-authorised by change management and in accordance with the Authority's operational Change Management Policies and Processes, that has an accepted and established Procedure to provide a specific change requirement;
Supplier Major Incident Manager	means the Supplier's representative responsible for ensuring that Major Incidents are resolved and closed within agreed timescales by the right group or team (acts as the main point of contact and manager of high priority Incidents, ensuring Incidents are managed and resolved with minimum impact to the business);
Supplier Management	means the management of Supplier-facing business processes throughout the lifecycle of the Agreement;
Technical Framework	means a structure intended to serve as a support or guide for Supplier listing the Authority's high-level technical solution principles;
Technology Refresh Policy	means the principles and/or rules that determine how frequently the Authority's IT assets (software and/or hardware) should be renewed;
Technology Refresh Service	means the Service by which the Supplier will renew the Authority Assets that will be undertaken in accordance with the Authority's Change Management Policies and Processes
Telephony Solution	means a Service provided by a Supplier that enables the Authority to electronically transmit voice information for the purposes of Incident raising;
Test Environment(s)	means the associated hardware, software and network configuration required to prove a discrete Test requirement;
Test Product Re-Use Library	means a library produced by the Supplier containing Test modules, Test Plans, Test documents, Test scripts, Test data, common re-usable packaged application tools and other similar materials that have been used in previous Projects and which are likely to be re-usable in the future;
Transformed Sites	means sites that have undergone a specific Transformation Project;
Video Conference Endpoints	means the hardware that sends and receives the video and audio required to deliver a face-to-face video meeting;
White Listed Categories	means a list of URL addresses or defined categories of URLs in respect of each of which the Authority has instructed the Supplier to allow access via the internet access service; and
Wide Area Network or WAN	means a computer network that spans a large geographical area and/or connects two or more Local Area Networks.

SCHEDULE 2.1 (SERVICES DESCRIPTION)

PART B – SUPPLIER SOLUTION

1. INTRODUCTION

1.1 This Part B describes how the Supplier Solution shall comply with all of the Service Requirements set out in Part A of this Schedule.

1.2 The Supplier shall provide the Services without any disruption to the Authority and its End Users, save as otherwise set out in the Agreement.

1.3 The Supplier shall supply the Services to meet the Service Requirements.

1.4 A summary of the Supplier Solution is set out below under this Paragraph 1.4.

2 SCOPE

2.1 The Parties acknowledge and agree that where there are Service Requirement ID references within the relevant element of the Supplier Solution, such Service Requirement ID references indicate which specific Service Requirement(s) are being fulfilled. Notwithstanding the foregoing, this shall not prevent such relevant element of the Supplier Solution (including the interpretation thereof) fulfilling other Service Requirement(s) (other than the specific Service Requirement(s) identified in the Service Requirement ID references in the Award Questionnaire responses), as applicable.

3 SUPPLIER SOLUTION

3.1 The Supplier Solution is set out in Annex 1 of this Schedule.

ANNEX 1: SUPPLIER SOLUTION

AQ1.2 Paragraph 5: **Service, Process and Technical Boundaries between IMS3 and IMS4**

SCHEDULE 2.2

PERFORMANCE LEVELS

SCHEDULE 2.2

PERFORMANCE LEVELS

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"Available"	has the meaning given in Paragraph 1.1 of Part C of this Schedule
"E-VIP End User"	refers to those VIP End Users who are nominated by the Authority and notified to the Supplier as requiring the fastest Resolution targets as more particularly described in KPI-11;
"End User"	any person authorised by the Authority to use the IT Environment and/or the Services;
"Non-Available"	in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available;
"Performance Monitoring Report"	has the meaning given in Paragraph 1.2(a) of Part B of this Schedule;
"Performance Review Meeting"	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 of this Schedule;
"Repeat KPI Failure"	has the meaning given in Paragraph 3.4 of Part A of this Schedule;
"Resolution"	has the meaning given in Paragraph 5.2 of Part C of this Schedule;
"Satisfaction Survey"	has the meaning given in Paragraph 9.1 of Part C of this Schedule;
"Service Availability"	has the meaning given in Paragraph 2 of Part C of this Schedule;
"Service Desk"	the single point of contact help desk set up and operated by the Supplier for the purposes of this Agreement;
"Service Downtime"	any period of time during which any of the Services are not Available;
"Security Incident"	is more particularly described in the table contained in Paragraph 5.8 of Part C to this Schedule, and includes Breaches of Security, as defined in Schedule 2.4 (*Security Management*);
"Service Requests"	means a request from an End User or an End User's authorised representative for information, advice, a Standard Change, or access to a service that will initiate a service action which has been agreed as a part of service delivery including the service requests listed in Annex 2 to this Schedule.

"Service Improvement Fund" or "SIF"	refers to a fund which is linked to exceptional Supplier performance against SIF KPIs, as more particularly described in Paragraph 5 of Part B to this Schedule;
"SIF KPIs"	refers to those specific KPIs, as per Annex 4 of this Schedule, that will be used by the Authority to determine whether exceptional performance has been achieved by the Supplier;
"System Response Time"	has the meaning given in Paragraph 3.1 of Part C of this Schedule; and
"VIP End User"	refers to those End Users determined by the Authority and notified to the Supplier as entitled to priority Resolution targets over End Users for the Services.

2 PRINCIPLES

2.1 The Authority has created a Service Credit regime set out in this Schedule which is intended to:

(a) incentivise exceptional Supplier performance in the delivery of the Services;

(b) ensure that the Services are, and remain, of a consistently high quality to meet the Authority Requirements;

(c) enable the Authority and the Supplier to respectively measure and recognise the impact, damage and/or loss resulting from the Supplier's failure to deliver the levels of Service it has agreed; and

(d) compensate the Authority for continued, or repeated, poor Supplier performance (where appropriate), without prejudice to remedies provided elsewhere in this Agreement.

2.2 Performance Indicators and Service Credit measures and mechanisms shall be subject to such detailed additions and amendments as the Authority deems necessary to make them operate both efficiently and effectively. To the extent that a mechanism or measure does not operate clearly or logically, the Authority shall be entitled to determine how it should operate based on the underlying principles behind the given mechanism, or measure, or (if this is not capable of determination) as the Authority shall determine acting reasonably.

3 APPLICATION

3.1 Subject to Paragraph 2.3 of Part A of this Schedule below, the provisions in this Schedule shall apply in their entirety for each Service during the Term.

3.2 Shared KPIs and SPIs (where applicable) shall apply to the Services for which one or more of the relevant Operational Service Commencement Dates have occurred.

PART A: PERFORMANCE INDICATORS AND SERVICE CREDITS

1 PERFORMANCE INDICATORS

1.1 Annex 1 sets out the Key Performance Indicators ("**KPIs**") and Subsidiary Performance Indicators ("**SPIs**") which the Parties have agreed shall be used to measure the performance of the Services by the Supplier during the Term.

1.2 KPIs and SPIs are divided into:

(a) specific KPI Targets, that apply only to the Supplier, and attract Service Points which can be converted to Service Credits paid to the Authority by the Supplier in accordance with Schedule 7.1 (*Charges and Invoicing*);

(b) specific SPI Targets, that apply only to the Supplier, for which Service Credits apply only when an SPI is promoted to a KPI under sub-Clause 7.7(b) (*Changes to Performance Indicators and Service Credits*);

(c) shared KPI Targets, that may apply both to the Supplier and Other Suppliers, subject to any agreed Service Credit apportionment;

(d) shared SPI Targets, that may apply both to the Supplier and Other Suppliers only when the Authority promotes an SPI to a KPI under sub-Clause 7.7(b) (*Changes to Performance Indicators and Service Credits*); and

(e) limited, specific compound KPIs that comprise several business affecting, weighted measures. These compound KPIs are identified in those tables labelled as such in Annex 3 to this Schedule

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

1.4 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5 of Part A of this Schedule and the weightings applied in Annex 3.

1.5 Service Credits shall be calculated for each Service Period, in accordance with the formula contained in Paragraph 2.2 to Part C of Schedule 7.1 (*Charges and Invoicing*) and, where Service Credits are paid, Service Credits shall:

(a) not apply to Service Request response time failures (unless the provisions of Paragraph 7.6 of Part B to this Schedule apply, or KPI-08 applies);

(b) not be the Authority's exclusive financial remedy for any Performance Failure (as stated in Clause 7.3 (*Performance Failures*)); but

(c) be subject to the Service Credit Cap.

1.6 The Service Credit Cap shall be apportioned against the relevant KPI in accordance with the Service Points incurred by the Supplier in the relevant Service Period, and for the compound KPIs, such apportionment shall be allocated in accordance with the table in Annex 9 of Schedule 7.1 (*Charges and Invoicing*). The Authority may vary the amount of Service Credits that can accrue against each applicable KPI during any Service Period, provided that such accrued Service Credits do not exceed the Service Credit Cap.

1.7 The weighting to be applied to Service Credits payable for each KPI Failure shall be as set out in Annex 3.

1.8 Notwithstanding any other provisions of this Schedule or elsewhere in the Agreement, the Parties acknowledge and agree that in relation to any Services which are only partially switched on and as such are not 100% operational up to Milestone M2 (Service Desk Go Live), including Early Start Services up to Milestone M2 (Service Desk Go Live), Service Credits shall not accrue or be applied in respect of such partially switched on Services.

2 SERVICE POINTS

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

2.2 Subject to Paragraph 2.3 of Part A of this Schedule, if the level of performance of the Supplier during a Service Period is below the Target Performance Level in respect of a KPI, Service Points shall accrue to the Supplier in respect of that KPI as set out in Paragraphs 2.3 and 2.4 below.

2.3 The level of performance of the Supplier will be measured, and therefore the performance monitoring obligations on the Supplier in Paragraph 1.1 of Part B will commence, from the Operational Service Commencement Date, and the provisions of Paragraph 2.2 of this Part A above (with respect to the accrual of Service Points and deductions of Service Credits by the Supplier) will apply.

2.4 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 3 to this Schedule, unless the KPI Failure is a Repeat KPI Failure when the provisions of Paragraph 3.2 of Part A of this Schedule shall apply.

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES

3.1 This Paragraph 3 to Part A of this Schedule applies to repeated KPI Failures, other than Service Availability and Severity 1 and 2 Incidents, and the Supplier shall provide lead support in the relevant response (supported by Other Suppliers, where necessary).

Repeat Failures

3.2 Where the same KPI or SPI is not met by the Supplier in any three (3) Service Periods out of six (6) Service Periods (on a rolling six (6) Service Period basis), the Supplier shall submit an Exception Report in conjunction with any Other Supplier to the next meeting of the relevant Working Group following the third KPI or SPI Failure. The Supplier shall ensure that such Exception Report includes root cause analysis and rectification activity, including at least the information set out in Paragraph 1.3(e) and 1.3(g) of Part B of this Schedule below. The Authority shall then determine whether a Rectification Plan is required and, where required, the Supplier shall comply with the Rectification Plan Process. The scope and format of all Rectification Plans shall be defined and documented by the Supplier in accordance with the Authority's Service Management Policies and Processes and reflected in the Supplier's Service Management Operating Procedures.

3.3 Failure by the Supplier to improve the relevant KPI or SPI performance shall constitute a Rectification Plan Failure, and therefore a Supplier Termination Event.

3.4 If a KPI Failure occurs in respect of the same KPI in any two consecutive Service Periods, the second and any subsequent such KPI Failure shall be a "**Repeat KPI Failure**".

3.5 A ratcheting mechanism will apply to increase the number of Service Points that accrue to the Supplier in respect of each Repeat KPI Failure.

3.6 The ratcheting mechanism for Repeat KPI Failures shall operate by applying a multiplier to the number of Service Points that would normally accrue to the Supplier in respect of an initial failure to meet a KPI, as follows:

Number of Repeat Failures	Multiplier
0	1.00
1st Repeat Failure	1.25
2nd Repeat Failure	1.50
3rd Repeat Failure	2.00
4th Repeat Failure	2.50
5th and each subsequent Repeat Failure	3.00

Related KPI Failures

3.7 If any specific KPIs 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 PLANNED MAINTENANCE

4.1 The Supplier shall not disrupt the provision of the Services for any purpose, and there shall be no relief or exclusion for the Supplier from the Service Points and Service Credits as a result of any Planned Maintenance activity.

4.2 The Supplier shall ensure that Planned Maintenance takes place only between the hours and on the days specified in the Maintenance Schedule (and, in any event, outside of the Support Hours unless the Authority expressly agrees) and is carried out in accordance with the Maintenance Schedule;

4.3 The Supplier shall give the Authority a minimum of 10 Working Days' (or such shorter period as is necessary to ensure the integrity of the Services) notice of its requirements in relation to Planned Maintenance (including timing, duration and measures to minimise business disruption)

4.4 The Supplier shall obtain prior written approval from the Authority for each instance of Planned Maintenance.

5 CONVERSION

Paragraph 2 to Part C of Schedule 7.1 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits. The weighting applicable to Service Credits is as set out in Annex 3.

PART B: PERFORMANCE MONITORING

1. PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 As part of the high level design to be provided by the Supplier in connection with Milestone M1 (High Level Design and detailed planning complete), the Supplier shall provide a draft performance management system (in written, report form) to the Authority (including the tools and methods it proposes to use to monitor and report on the Supplier's performance against the Performance Indicators). The draft performance management system report shall be designed and resourced sufficiently to:

(a) ensure that the Authority is able to determine and measure accurate, complete and transparent Supplier performance against the Performance Indicators;

(b) ensure that the Service Credit regime may be implemented comprehensively, accurately, and without Dispute;

(c) ensure that the ITSM Product will meet the reporting requirements set out in this Part B to this Schedule; and

(d) provide a clear picture of performance such that the Authority is able to report accurately and clearly to other Service Recipients and End Users.

1.2 Following the end of each Service Period, the Supplier shall provide a report to the Authority which summarises the Supplier's performance**:**

(a) against each of the Performance Indicators as more particularly described in Paragraph 1.3 of this Part B (the "**Performance Monitoring Report**"); and

(b) over the relevant Service Period as more particularly described in Paragraph 1.4 of this Part B (the "**Balanced Scorecard Report**").

Performance Monitoring Report

1.3 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each KPI and SPI, the actual performance achieved over the Service Period, and that achieved over the previous 3 Service 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;

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

(e) for any Material KPI Failures or Material SPI Failures occurring during the Service Period, the cause of the relevant KPI Failure or SPI 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) the conduct and performance of any agreed periodic Tests that have occurred, such as the annual failover Test of the Service Continuity Plan;

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

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

(m) details relating to the Supplier's governance of resource demand and capacity management.

Information in respect of previous Service Periods

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

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

(c) the conduct and performance of any agreed periodic Tests that have occurred in such Service Period such as the annual failover Test of the Service Continuity Plan; and

Information in respect of the next Quarter

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

Balanced Scorecard Report

1.4 The Balanced Scorecard Report shall be presented in the form of an online accessible dashboard and, as a minimum, shall contain a high-level summary of the Supplier's performance over the relevant Service Period, including details of the following:

(a) financial indicators;

(b) the Target Performance Levels achieved;

(c) behavioural indicators;

(d) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;

(e) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice;

(f) Milestone trend chart, showing performance of the overall programme;

(g) sustainability and energy efficiency indicators, for example energy consumption and recycling performance; and

(h) Social Value (as applicable).

1.5 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.6 below.

1.6 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 Meetings shall (unless otherwise agreed):

(a) take place within five (5) Working Days 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

(c) be attended by the Supplier Representative and the Authority Representative.

1.7 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 SPI Failure.

2. PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and Records (including Service Desk Records, Supplier Personnel Records, timesheets, training programmes, Supplier Personnel 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 (through any project board or Working Group) 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 of this Part B 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 (as well as historic Performance Monitoring Reports and historic Balance Scorecard Reports) 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

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

3.2 Where a Dispute arises between the Parties as to whether a Performance Indicator has been achieved, the Parties shall follow the procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*).

4 CHANGES TO PERFORMANCE MEASURES

4.1 The Authority may, at its discretion, conduct a review of any or all of the measurement indicators set out in this Schedule which are used to measure the Supplier's performance under this Agreement, including the Performance Indicators, Target Performance Levels, Service Periods, Service Credits, Service Points and Service Credit Cap (together, "**Performance Measures**") in accordance with Clause 7.7 (*Changes to Performance Indicators and Service Credits*).

4.2 Clause 7.7(b) (*Changes to Performance Indicators and Service Credits*) sets out the mechanism by which the Authority may convert one or more KPIs into SPIs, or SPIs into KPIs (as applicable).

4.3 Where any SPI is promoted to a KPI, then all rights and remedies attributable to KPIs shall be available to the Authority in respect of that converted SPI, including the right to seek remedies for a Material KPI Failure.

4.4 Where the Supplier consistently achieves a KPI which was promoted from an SPI, the Authority may (at its discretion) agree to demote the KPI back to an SPI.

4.5 The Authority shall use the Performance Monitoring Reports provided pursuant to this Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period, and the weighting to be applied to each Service Credit, as set out in Annex 3.

5 SERVICE IMPROVEMENT FUND

5.1 Where the Supplier:

(a) meets or exceeds all of the SIF KPI Targets for the SIF KPIs; and

(b) does not accrue any Service Points;

over the same Service Period, this amounts to "exceptional Supplier performance" and the Authority agrees to pay an amount into the SIF in accordance with Paragraph 5.2 of this Part B.

5.2 The Authority shall contribute £[redacted] (incl. VAT) per month into the SIF for every month that the Supplier satisfies the criteria listed in Paragraph 5.1 of this Part B.

5.3 The Authority shall hold all monies in the SIF which shall be available for use by the Authority at its sole discretion to commission the Supplier to deliver future projects and Work Requests. The Supplier shall proactively suggest appropriate future projects and Work Requests to be carried out using the SIF, subject always to the Approval of the Authority.

5.4 Payments distributed to the Supplier as consideration for work commissioned from the Authority and remunerated through the SIF shall not be considered for the purposes of calculating the Supplier's Maximum Permitted Profit Margin in the Annual Contract Report.

5.5 The SIF shall be administered by the IT Programme Board in accordance with the terms of reference contained in Schedule 8.1 (*Governance*).

5.6 Any amounts remaining in the SIF at the termination or expiry of this Agreement shall remain with the Authority.

PART C: RESPONSE TIMES

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); and

(c) all Performance Indicators other than Service Availability are above the KPI Target Performance Levels.

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:

$$\text{Service Availability \%} = \frac{(MP-SD)\times 100}{MP}$$

where:

MP = total number of minutes within the relevant Service Period; and

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

2.2 When calculating Service Availability in accordance with this Paragraph 2, Service Points shall not accrue for any Service Downtime due to Emergency Maintenance undertaken by the Supplier where the Supplier can demonstrate to the Authority (acting reasonably) that the Supplier was not the cause (in whole or in part) of the fault which required such Emergency Maintenance.

2.3 Any maintenance undertaken by the Supplier over eight (8) hours in any Service Period shall automatically be deemed to be Service Downtime.

3 RESPONSE TIMES

3.1 The "**System Response Time**" is the round trip time taken to process a message or request of the IT Environment and/or the Services, and shall be measured from the moment the last packet of data which relates to a particular message is received at the external interface of the IT Environment until a response is generated and the first block of data leaves the external interface (including, for the avoidance of doubt, the time taken for any necessary processing).

3.2 The Supplier System Response Time shall be the average System Response Time measured over the course of a Service Period.

4 SERVICE DESK RESPONSE TIMES

4.1 The Service Desk shall be the main point of contact for End Users to log Incidents and Service Requests, as more particularly described in Paragraph 19 of Part A of Schedule 2.1 (*Services Description*).

4.2 Measurement of Service Desk response times will be based on the time taken for a Service Desk operative to answer a call. Calls receiving an automated response or placed into a queuing system shall be deemed not to have been answered.

4.3 The Supplier shall monitor the Service Desk response times and shall provide the results of such monitoring to the Authority in accordance with the provisions of Part B of this Schedule.

5 INCIDENT RESOLUTION AND FIX TIMES

5.1 The Supplier shall manage and oversee the lifecycle of all Incidents, including First Line Support, Incident triage through to Resolution, consulting with the relevant End User throughout the Fix Time.

5.2 The "**Fix Time**" of an Incident is the period from the time that the Incident has been reported to the Supplier to the point of its Resolution and "**Resolution**" means in relation to an Incident either the:

(a) root cause of the Incident has been removed and the Services are being provided in accordance with the Services Description and Performance Indicator; or

(b) Authority has been provided with a workaround in relation to the Incident deemed acceptable by the Authority.

5.3 Incidents shall be assigned a Resolution Severity by the Supplier based on their severity level set out in the table in Paragraph 5.7 of this Part C below. However, the Authority reserves the right to assign a different Incident Severity (acting reasonably), which shall be accepted by the Supplier.

5.4 Fix Times for Severity 3 Incidents, Incident shall be measured in Operational Hours only.

5.5 Fix Times for Severity 1 Incident and Severity 2 Incidents shall be measured 24x7.

5.6 The Supplier shall measure Fix Times as part of its service management responsibilities and report periodically to the Authority on Fix Times as part of the Performance Monitoring Report.

5.7 For the purposes of Paragraph 5 of this Part C, the following expressions shall have the meanings set opposite them below:

"Support Hours"	means the Operational Hours of 07:00 – 22.00 on all Working Days;
"Operational Hours"	means, in relation to any Service, the hours for which that Service is to be operational as set out in Part A of Schedule 2.1 (*Services Description*);
"Service Hours"	refers to the period when the Services are Available to the End Users, including all Operational Hours and Support Hours;
"Incident"	refers to any interruption to any aspect of the Services, including any reported occurrence of a failure by the Supplier to deliver any part of the Services in accordance with the Authority Requirements or the Performance Indicators;

Severity 1 Incident or **"Severity 1"** **(Extensive)**

an Incident which, in the reasonable opinion of the Authority:

(a) constitutes a loss of the Service which prevents a large group of End Users from working, or any VIP End User or e-VIP End User from completing their work;

(b) has a critical impact on the activities of the Authority, including mission critical equipment or services;

(c) causes significant financial loss and/or disruption to the Authority;

(d) may damage public confidence in the Government;

(e) is, or is suspected of being, concerted, repeating, targeted efforts to cause harm to systems or Authority Data;

(f) may cause loss of an information bearing asset which has not been verified as in a secure state; or

(g) results in any material loss or corruption of Authority Data;

Non-exhaustive examples:

- a loss of power to a data centre causing failure of Services;
- unavailability of the protective monitoring service that prevents accounting items from being collected, processed, alerted or reported, and for which such related data is permanently lost; or
- a failure of the Services to provide End User authentication service;

Severity 2 Incident or **"Severity 2"** **(Significant)**

an 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;

(b) impact a smaller group of End Users and disrupt non-essential services and/or breaches network security policy;

(c) affect the reputation of Government bodies and services;

(d) have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available; or

(e) cause a financial loss and/or disruption to the Authority which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Failure;

Non-exhaustive examples:

- corruption of organisational database tables;
- targeted attacks attempting to cause harm; or
- loss of ability to update Authority Data.

Severity 3 Incident or "**Severity 3" (Moderate)**

an Incident which, in the reasonable opinion of the Authority has the potential to:

(a) have a major adverse impact on the activities of the Authority which can be reduced to a moderate adverse impact due to the availability of a workaround acceptable to the Authority; or

(b) have a moderate adverse impact on the activities of the Authority;

Non-exhaustive example:

- inability to access data for a class of customers;
- unsuccessful denial-of-service attacks;
- majority of network monitoring alerts;
- non-targeted Breaches of Security;
- loss of an information bearing asset where Authority Data is held in a secure state; and
- behavior recognised as suspicious without supporting evidence;

Security Incidents

5.8 Subject to Paragraph 5.10 of this Part C, the Supplier shall assign Security Incidents and Breaches of Security a severity level in accordance with the following table:

Severity Level	Definition
1 (Extensive)	▪ A Security Incident that causes, or may cause, the degradation of vital services for a large number of End Users and involves a serious Breach of Security and/or affects mission critical equipment or services and/or damage public confidence in the Government; or ▪ A Security Incident that is, or is suspected to be, a concerted, repeating, targeted, effort causing harm to confidentiality, integrity or availability of ICT systems or data; or ▪ Loss of an information bearing asset where it has not been verified that the data is in a secure state.
2 (Significant)	▪ A Security Incident that is not Critical and which impacts, or may impact, a smaller group of End Users and disrupts non-essential services and/or breaches network security policy and/or affects the reputation of Government bodies and services; or ▪ A Security Incident that is, or is suspected to be, a targeted attack attempting to cause harm to confidentiality, integrity or availability of ICT systems or data.
3 (Moderate)	▪ A Security Incident that is not Critical or Significant and does not typically impact IT services and includes instances such as unsuccessful denial-of-service attacks or the majority of network monitoring alerts; or ▪ A Security Incident that is likely to be non-targeted; or ▪ Loss of an information bearing asset where the data is in a secure state; or ▪ Instances where activity or behaviour is recognised as suspicious but lack supporting evidence.

5.9 Where a Security Incident occurs, the target Resolution times applicable to the Supplier are set out in Annex 1 below:

5.10 The Authority reserves the right to determine a different severity level to a Security Incident, and the Supplier and Other Suppliers shall accept and work to the severity level assigned by the Authority.

6 VIP END USERS

6.1 [redacted]

6.2 [redacted]

6.3 [redacted]

6.4 [redacted]

[redacted] [redacted]

[redacted] [redacted]

7 SERVICE REQUEST FULFILMENT

7.1 The Supplier shall provide end to end management of the fulfilment of Service Requests and shall work with Other Suppliers and to fulfil Service Requests, as set out in Part A of Schedule 2.1 (*Services Description*).

7.2 Service Requests shall be fulfilled in accordance with the relevant fulfilment time as set out in the Service Catalogue contained in Annex 2. Where there is no fulfilment time stated in the Service Catalogue, the fulfilment time shall be agreed between the Authority and the Supplier on a case by case basis. The Authority has identified key Service Requests as measured catalogue items, as are set out in Annex 1 and Annex 2 of this Schedule.

7.3 The Authority shall be entitled to, in agreement with the Supplier (such agreement not to be unreasonably withheld or delayed), add further Service Requests at its discretion and without amendment to the Charges.

7.4 Where a Service Request involves Other Suppliers in its fulfilment, any time that is exclusively due to the activities of the Other Suppliers shall be excluded from the calculation of the Supplier's performance against the Performance Indicators.

7.5 The Authority may determine additional Service Requests without amendment to the Charges.

7.6 Where a Service Request involves Other Suppliers in its fulfilment, any time that is exclusively due to the activity of the Other Supplier(s) (but not including Sub-contractors) shall not be calculated as part of the Supplier's performance.

7.7 The Authority may promote certain Service Requests to KPIs and assign Service Points individually, where appropriate (acting reasonably).

8 VULNERABILITY MANAGEMENT

8.1 Following the IT Health Check carried out pursuant to Schedule 2.4 (*Security Management*), the Supplier shall provide ongoing vulnerability management as required by Part A of Schedule 2.1 (*Services Description*).

8.2 For each identified vulnerability, the Supplier shall specify within its Vulnerability Correction Plan the timescale for implementation of the Resolution to the identified vulnerabilities, or such shall be as specified in Paragraph 9 of Annex A1 (*Vulnerabilities and Corrective Action*) to Schedule 2.4 (*Security Management*).

9 SATISFACTION SURVEYS

9.1 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 KPIs and SPIs; and/or

(b) other suggestions for improvements to the Services.

9.2 The Authority shall reflect in the Balanced Scorecard Report any aspects of the Supplier's performance of the Services which the responses to the Satisfaction Surveys reasonably suggest are not meeting the Services Description.

10 AUTHORITY DOCUMENT MANAGEMENT SYSTEM COMPLETENESS

The Authority Document Management System shall be complete where all of the information required under Schedule 8.4 (*Reports and Records Provisions*) Annex 3 (*Documentary Deliverables and Storage Location*) has been uploaded to the Authority Document Management System in accordance with Paragraph 3 of that Schedule.

ANNEX 1: KPIs and SPIs

The KPIs and SPIs that shall apply to the Operational Services are set out in this Annex 1:

1. Service Desk and End User Compute – KPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	KPI Target Performance Level	Publishable Performance Information to the Cabinet Office
KPI-01	Service Desk Customer Satisfaction	Service Desk specific customer satisfaction on a scale of 1-5 measuring (a) the delivery and (b) the customer experience. The percentage of respondents to score a total of eight (8) or above on a monthly basis.	= (A/B)*100 A. The number of responses scoring eight (8) or above during a given Supplier customer satisfaction survey initiative. B. The total number of responses received during the given survey initiative period.	Monthly	≥ 85%	Yes
KPI-02	First Time Fix (FTF) of Resolvable Calls received by the Service Desk, Tech Hub and Virtual Tech Hub	The percentage of resolvable calls resolved and closed on the first contact by the Service Desk Agent, the Tech Hub or Virtual Tech Hub agent (i.e. Agent does not transfer, escalate change Severity of call or initiate or request a call back).	= (A/B)*100 A. The sum of all resolvable calls received by the Service Desk, the Tech Hub and the Virtual Tech Hub at first contact during the Service Period. B. The sum of all resolvable calls resolved at first contact by the Service Desk, the Tech Hub and the Virtual Tech Hub during the Service Period.	Monthly	≥ 90%	Yes
KPI-03	Non-automated Service Desk Agent Responses to Chat Channel Contact	Initial non-automated Service Desk Agent response to chat channel contact within 45 seconds or less.	= (A/B)*100 A. The total number of chat channel contact requests initiated by the End User or referred from a chatbot that were answered by an agent within 45 seconds.	Monthly	≥ 90% within 45 seconds	No

			B. The total number of chat channel contact requests received by the Service Desk.			
KPI-04	Correct Allocation of a Ticket to a Resolver Group	The percentage of tickets assigned to the correct Resolver Group by the Service Desk (first time round).	= (A/B)*100 A. The number of tickets assigned to the correct Resolver Group, first time round. B. The total number of tickets that are assigned to Resolver Groups.	Monthly	≥ 95%	No
KPI-05	Incident Resolution Time (Severity 1 Extensive)	The number of Severity 1 Incidents that are Resolved within the specified timeframe, for all those Severity 1 Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers to resolve it.	= # (number) of Severity 1 Incidents	Monthly	100% of Severity 1 Incidents within 4 Service Hours	No
KPI-06	Incident Resolution Time (Severity 2 Significant)	The percentage of Severity 2 Incidents that are Resolved within the specified timeframe, for all those Severity 2 Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other Suppliers to resolve it.	= (A/B)*100 A. The sum of all Severity 2 Incidents Resolved within the specified timeframe during the Service Period. B. The total number of Severity 2 Incidents Resolved in the Service Period.	Monthly	Severity 2 ≥ 95% within 8 Support Hours	No
KPI-07	Incident Resolution Time (Severity 3 Moderate)	The percentage of Severity 3 Incidents that are Resolved within the specified timeframe, for all those Severity 3 Incidents where the Service Desk has identified that the resolution of the Incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with Authority's Other	= (A/B)*100 A. The sum of all Severity 3 Incidents Resolved within the specified timeframe during the Service Period. B. The total number of Severity 3 Incidents Resolved in the Service Period.	Monthly	Severity 3 ≥ 90% within 30 Support Hours	No

		Suppliers and Other Service Providers to resolve the Incident.				
KPI-08	Severity 1 Volume	The number of Severity 1 Incidents raised in a Service Period.	= number of Severity 1 Incidents in a Service Period	Monthly	No more than two (2) Severity 1 Incidents in a Service Period.	No
KPI-09	Service Request Fulfilment	Time to fulfil Service Requests in accordance with the Service Catalogue. The percentage of Service Requests for which the Supplier is responsible which are implemented successfully and within the stated timeframe for that specific request as defined within the relevant Service Catalogue (see Paragraph 7.2 of Part C of this Schedule for individual catalogue item KPIs).	= (A/B)*100 A. The sum of all service requests for which the Supplier is responsible which are implemented successfully and within the stated timeframe for that specific request as defined in the Service Catalogue during the Service Period. B. The sum of all service requests that the Supplier is responsible for implementing during that Service Period.	Monthly	≥ 99%	Yes
KPI-10	Service Desk & ITSM Product Availability	The percentage availability across all contact methods, channels, and operational capability of the Service Desk and ITSM Product.	= (A/B)*100 A. The Support Hours the Service Desk and ITSM Product is available. B. The total Support Hours the Service Desk and ITSM Product is meant to be available.	Monthly	≥ 99.9%	No
KPI-11	[redacted]					

		to work with Authority's Other Suppliers to resolve the Incident or fulfil the Request.				
KPI-12	Communication to the Authority of all types of Severity 1 and Severity 2 Incidents (including Security Incidents)	Percentage of all types of Severity 1 and Severity 2 Incidents where the time to inform the Authority is within 15 minutes of the Incident being identified as a Severity 1 or Severity 2 Incident.	= (A/B)*100 A. The total number of Severity 1 and Severity 2 Incidents where the time to inform the Authority is within 15 minutes of the Incident being identified as a Severity 1 or Severity 2 Incident B. The total number of Severity 1 and Severity 2 Incidents.	Monthly	100%	No
KPI-13	Percentage of estate and infrastructure with latest revision Security Patches Implemented	Percentage of the in-scope estate and infrastructure services covered by the latest revision of security patches successfully implemented in accordance with the Authority's Information Security Policies and Standards.	= (A/B)*100 A. The number of in-scope estate and infrastructure services with the latest revision security patches updates implemented in a Service Period. B. The total number of in-scope estate and infrastructure services with the latest revision security patches updates required to be implemented in a Service Period.	Monthly	100%	No
KPI-14	Service Desk Average Call Answer Time	Percentage of calls answered in less than 60 seconds. The average time (in seconds) taken by the Service Desk to answer calls (following any automated messages).	= (A/B)*100 A. The total number of calls answered by Service Desk Agents in under 60 seconds. B. The total number of calls received, minus the number of calls abandoned before 60 seconds after the automated message (IVR).	Monthly	≥ 90%	No
KPI-15	Root Cause Analysis Severity 1 & Severity 2	Proportion of Severity 1 Root Cause Analysis completed by the Supplier within 7 Days from the closure of the Severity 1 event and 10 Working Days from the closure of the Severity 2 event. Initial RCA for a Severity 1 and a	= (A/B)*100 A. The number of Severity 1 and Severity 2 RCAs delivered by the Supplier within 2, 7 and 10 Working Day targets (for Initial RCA (Severity 1) Complete RCA (Severity 1) and Complete RCA (Severity 2)	Monthly	≥95% Initial RCA – 2 Working Days (Severity 1 & Severity 2) Complete	No

		Severity 2 within 2 days.	respectively). B. The total number of Severity 1 and Severity 2 RCAs requested of the Supplier via the Problem Management.		RCA - 7 Working Days (Severity 1) Complete RCA - 10 Working Days (Severity 2)	

2. Service Desk and End User Compute – SPIs

No.	KPI Performance Criterion	Description	Formula	Frequency of Measurement	SPI Target Performance Level	Publishable Performance Information
SPI-01	Respond to Contract Change Requests	Percentage of Contract Change Requests to the Supplier by the Authority that have a quote completed and returned to the Authority that are capable of acceptance by the Authority, within the allotted key performance indicator for the size/category of change. - Small Works within 3 Working Days - Repeatable within 3 Working Days - Project within 10 Working Days (with a ROM within 5 Days) - Large Project within 20 Working Days (with ROM within 10 Days)	= (A/B)*100 A. The number of Contract Change Requests for a change by size category that are completed to their respective category SPI. B. The total number of Contract Change Requests by size category that were requested of the STP by their respective size category.	Monthly	≥ 98%	No
SPI-02	Capacity Buffer Threshold Management	To ensure that the capacity buffer Threshold for Supplier provisioned services is maintained for the relevant Services through the	Capacity buffer threshold management for Supplier provisioned Services shall be calculated as follows:	Monthly	100%	No

		provision of additional capacity within the required timeframes.	Number of Authority approved capacity fulfilment requests as a result of a capacity buffer threshold breach event actioned and provisioned within six (6) weeks of the capacity buffer threshold breach event (excluding the time taken by Authority to provide any approvals) Number of capacity fulfilment requests as a result of a capacity buffer threshold breach event generated and which are approved by the Authority X 100 = capacity management fulfilment %			
SPI-03	Emergency Operational Change Request Levels	Percentage of Supplier Contract Change Requests categorised as Emergency, in the last month in production	= (A/B)*100 A. The number of Emergency Change Requests implemented in the month. B. The total number of Emergency Change Requests implemented in the month.	Monthly	≤3%	No
SPI-04	Percentage of Supplier Knowledge Articles for use by the Service Desk updated within agreed timescales	Percentage of Supplier Knowledge Articles, for use by the Service Desk, updated within 24 Support Hours, where an inaccuracy has been identified by any Party and reported to the Supplier.	N/A	Monthly	100%	No
SPI-05	Failed Changes	To monitor and report on the number of requests relating to Operational Changes which are scheduled for implementation by the Supplier, but which are cancelled, failed and/or backed out.	= Number Total number of scheduled requests relating to Operational Changes which are backed out (not implemented) in a month. = Percentage (A/B)*100 A. The number of scheduled Operational Changes backed out in a month. B. The total number of scheduled Operational Changes in the month in question.	Monthly	≤3%	No

SPI-06	Open Ticket older than 2 weeks	Percentage of open tickets that are over 2 weeks old and are not awaiting an action or dependency on another Supplier or the Authority.	= (A/B)*100 A. The number of open Tickets that are over 2 weeks old and not dependent on another Supplier or the Authority. B. The total number of open Tickets that are not dependent on another Supplier or the Authority.	Monthly	≤10%	No
SPI-07	Open Tickets older than 4 weeks	Percentage of open Tickets that are over 4 weeks old and are not awaiting an action or dependency on another Supplier or the Authority.	= (A/B)*100 A. The number of open Tickets that are over 4 weeks and not dependent on another Supplier or the Authority. B. The total number of open Tickets that are not dependent on another Supplier or the Authority	Monthly	0%	No
SPI-08	Severity Level 1 & 2 Incident Response Time	The percentage of all Severity 1 & Severity 2 Incidents that are allocated to the correct Resolver Group within the specified timeframe (10 minutes).	= (A/B)*100 A. The sum of all Severity 1 & Severity 2 Incidents allocated to the correct Resolver Group within the specified timeframe during the Service Period. B. The total number of Severity 1 & Severity 2 Incidents in the Service Period.	Monthly	≥ 95% in 10 minutes	No
SPI-09	Severity Level 3 Incident Response Time	The percentage of all Severity 3 Incidents that are allocated to the correct Resolver Group within the specified timeframe (30 minutes).	= (A/B)*100 A. The sum of all Severity 3 Incidents allocated to the correct Resolver Group within the specified timeframe during the Service Period. B. The total number of Severity 3 Incidents in the Service Period.	Monthly	≥ 95% in 30 minutes	No
SPI-10	Percentage of interactions of End Users with the Service Desk abandoned (all channels).	Percentage of interactions of End Users with the Service Desk abandoned irrespective of the channel used, in any given Service Period.	= (A/B)*100 A. The number of abandoned interactions in the Service Period. B. The total number of interactions in the Service Period. In measuring performance against this KPI the following items shall be disregarded and not included within the above calculation:	Monthly	≤5%	No

			Those calls abandoned in less than 30 seconds.			
SPI-11	Security Incidents	The percentage of Security Incidents that are Resolved within the specified timeframe within the Service Period, for all Security Incidents where the resolution of the incidents is the sole responsibility of the Supplier, and where the Supplier does not need to work with any Authority's Other Suppliers and Other Service Providers to resolve the Incident.	= (A/B)*100 A. The total number of all security incidents Resolved within a specified timeframe within the Service Period B. The total number of security incidents Resolved in the Service Period.	Monthly	100%	No
SPI-12	CMDB Operational Updates	Percentage of operational updates applied to CMDB within 2 Working Days from resolution of the relevant Incident or completion of the relevant Service Request, Request for Change.	= (A/B)*100 A. The total number of operational updates being applied within 2 Working Days from resolution of the relevant Incident or completion of the relevant Service Request, Request for Change B. The total number of CMDB operational updates requests.	Monthly	≥95%	No
SPI-13	Impact of Operational Changes	Percentage of Operational Changes scheduled in the Reporting Period where the Change causes an Incident.	= (A/B)*100 A. The total number of all Operational Changes scheduled in the reporting period where the Change causes an incident B. The total number of Operational Changes schedule in the reporting period.	Monthly	≤2%	No
SPI-14	Service Catalogue Updates	Percentage of Service Catalogue updates applied within two (2) Working Days from approved amendment	= (A/B)*100 A. The total number of service catalogue updates applied within 2 Working Days from the approved amendment B. The total number of service catalogue update requests.	Monthly	≥95%	No