



Ministry of
JUSTICE

Hosting

Schedule 1: Definitions

TABLE OF CONTENTS

1.	ACRONYMS.....	3
2.	DEFINITIONS.....	9

This Schedule contains some terms which do not appear in the Agreement but do appear in the Agreements of Other FITS Suppliers. These have been retained to assist the Hosting Supplier to understand the terminology that might be referred to by the Authority or Other FITS Suppliers from time to time. Where a term is included in this schedule but not used in the Agreement it shall have no legal effect for the Hosting Supplier.

1. ACRONYMS

Acronym	Definition
A2J	Access to Justice
ALB	Arms Length Body
AMIS	Availability Management Information System
AMS	Applications Maintenance and Support
APM	Application Performance Management
ATF	AMS Transition Function
ATIA	Architecture, Technology & Information Assurance
ATP	Authority To Proceed
BAU	Business As Usual
BC	Basic Check
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BIL	Business Impact Level
BSI	British Standards Institution
BU	Business Unit
CAB	Change Advisory Board
CAPEX	Capital Expenditure
CAPS	CESG Assisted Products Service
CAR	Consolidated Asset Register
CAS-T	CESG Assured Service – Telecoms
CCCJS	Co-ordinated Computerisation of the Criminal Justice System
CCN	Contract Change Note
CEDR	Centre for Effective Dispute Resolution
CESG	The National Technical Authority for Information Assurance, formerly known as the Communications-Electronics Security Group. See http://ncsc.gov.uk .
CFIA	Component Failure Impact Analysis
CI	Configuration Item
CIT	Component Integration Testing
CJS	Criminal Justice System
CJSE	Criminal Justice System Exchange
CJSM	Criminal Justice Secure Mail
CLAS	CESG Listed Adviser Scheme
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMO	Current Mode of Operation

CMS	Configuration Management System
COBIT	Control Objectives For Information And Related Technology
CoCo	Code of Connection
COTS	Commercial Off The Shelf
CPA	Commercial Product Assurance
CPNI	Centre for the Protection of National Infrastructure (CPNI). See http://www.cpni.gov.uk/
CPP	Contract Performance Point
CPU	Central Processing Unit
CRAMM	CCTA (Central Computing and Telecommunications Agency) Risk Analysis and Management Method
CSF	Critical Success Factor
CSI	Continual Service Improvement
CSIP	Continual Service Improvement Programme
CSOC	Cyber Security Operation Centre
CTAS	CESG Tailored Assurance Service
CTP	Consolidated Test Plan
CVSS	Common Vulnerability Scoring System
DCP	Detailed Cutover Plans
DCTF	Data Centre Transition Function
DDD	Detailed Design Document
DHCP	Dynamic Host Configuration Protocol
DIKW	Data-to-Information-to-Knowledge-to-Wisdom
DML	Definitive Media Library
DMP	Defect Management Process
DNS	Domain Name System
DR	Disaster Recovery
DRB	Defect Review Board
DRM	Digital Rights Management
DSB	Departmental Security Branch
DSL	Definitive Software Library
DTP	Detailed Transition Plan
DWP	Detailed Workstream Plan
E2E	End to End
ECAB	Emergency Change Advisory Board
ECMA	European Computer Manufacturers Association
EDRM	Electronic Document and Records Management
eGIF	e-Government Interoperability Framework
ELS	Early Life Support
EMS	Event Management System
EOL	End of Life
eSCM-CL	eSourcing Capability Model For Client Organizations
eSCM-SP	eSourcing Capability Model For Service Providers
ETF	EUCS Transition Function
EUCS	End-User Computing Services
FAQ	Frequently Asked Question
FCF	First Contact Fix
FCI	Filled Change Instruction
FCO	Filled Change Order
FITS	Future IT Sourcing
FMO	Future Mode of Operations

FOIA	Freedom of Information Act
FSAIT	FITS Service Desk & ITIL Transition
FTAF	FITS Transition Assurance Function
FTE	Full-Time Equivalent
FTF	First Time Fix
GMT	Greenwich Mean Time
GPG	Good Practice Guidelines
GSI	Government Secure Intranet
HIDS	Host Intrusion Detection Systems
HMG	His Majesty's Government
HOIT	Home Office IT
HQ	Head Quarters (of the Authority)
HR	Human Resources
HTF	Hosting Transition Function
IA	Information Assurance
IAMM	Information Assurance Maturity Model
IAO	Information Asset Owner
IBIS	Integrating Business and Information Systems - the IBIS Initiative - replaces the CCCJS
ICO	Information Commissioner's Office see http:// www.ico.gov.uk/
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IL	Impact Level
IM	Incident Management
IMAC(s)	Installations, Moves, Adds, Changes
IMS	Incident Management System
IP	Internet Protocol
IPR	Intellectual Property Rights
IR	Incident Record
IRR	Internal Rate Of Return
IS	Information System
ISG	IT Steering Group
ISM	Information Security Management
ISMS	Information Security Management System
ISP	Internet Service Provider
ISTQB	International Software Testing Qualifications Board see http://www.istqb.org
IT	Information Technology
ITHC	IT Health Check
ITIL	IT Infrastructure Library Framework
ITN	Invitation to Negotiate
ITSC	IT Service Continuity
ITSCM	IT Service Continuity Management
ITSM	Information Technology Service Management
ITT	Invitation To Tender
KEDB	Known Error Database
KPI	Key Performance Indicator
LAN	Local Area Network
M_o_R	Management Of Risk
MAC	Milestone Achievement Certificate
MAL	Master Application List

MI	Management Information
MoJ	Ministry of Justice
MSA	Master Service Agreement
MSP	Managing Successful Programmes
MTBF	Mean Time Between Failures
MTBSI	Mean Time Between Service Incidents
MTRS	Mean Time To Restore Service
MTTR	Mean Time To Repair
NCC	Nominated ESCROW agent: NCC Group Escrow Limited
NCSC	National Cyber Security Centre
NDPB	Non Departmental Public Body
NIDS	Network Intrusion Detection System
NOMS	National Offender Management Services
NPV	Net Present Value
NTF	Networks Transition Function
OAP	Other Authority Providers
OAT	Operational Acceptance Testing
OGC	Office of Government Commerce
OGD	Other Government Department
OLA	Operational Level Agreement
OPEX	Operational Expenditure
OWA	Operational Working Agreement
PBA	Pattern of Business Activity
PCI DSS	Payment Card Industry Data Security Standard
PD	Product Description
PGAS	The Pan Government Accreditation Service
PI	Performance Indicator
PIA	Privacy Impact Assessment
PID	Project Initiation Document
PIR	Post Implementation Review
PKI	Public Key Infrastructure
PLCM	Product Life Cycle Management
PMC	Protective Monitoring Controls
PMO	Project Management Office
PMS	Problem Management System
PMTF	Protective Monitoring Transition Function
POC	Proof of Concept
PoE	Power over Ethernet
PPD	Programmes and Project Delivery
PRINCE2	Projects IN Controlled Environments
PRISM	Post Release Implementation Support and Maintenance
PSN	Public Services Network
PSNA	Public Sector Network Authority
PTF	Print Services Transition Function
QoS	Quality of Service
R&I	Risks and Issues
RACI	Responsible, Accountable, Consulted, Informed
RAG	Red amber green
RAS	Remote Access Service
RBAC	Role Base Access Control
RFC	Request for Change

RfD	Request for Data
RfI	Request for Information
RFP	Request for Proposal
RFS	Request for Service
RG	Resolver Group
RMADS	Risk Management and Accreditation Documentation Set
ROI	Return On Investment
ROM	Rough Order of Magnitude
RPO	Recovery Point Objective
RSS	Rich Site Summary
RTO	Recovery Time Objective
SACM	Service Asset and Configuration Management
SAT	Service Acceptance Testing
SCAP	Security Content Automation Protocol
SCAT	Service Catalogue
SCD	Service Commencement Date
SDLC	Service Delivery Lifecycle
SDP	Service Design Package
SI	Service Integration
SIAM	Service Integration And Management
SIP	Service Improvement Plan
SIT	Systems Integration Testing
SKL	Service Knowledge Library
SKMS	Service Knowledge Management System
SL	Service Level
SLA	Service level agreements
SLAM	Service Level Agreement Monitoring
SLM	Service Level Management
SLP	Service Level Package
SLR	Service Level Requirement
SLT	Service Level Target
SMART	Specific, Measurable, Achievable, Relevant, and Time-Bound
SMIS	Security Management Information System
SMS	Short Message Service
SOA	Service Oriented Architecture
SoA	Statement of Applicability
SOC	Service Operation Centre
SOP	Standard Operating Procedure
SOR	Statement Of Requirements
SPF	Security Policy Framework
SPO	Strategy, Planning & Operations
SPoC	Single Point Of Contact
SPoF	Single Point Of Failure
SRO	Senior Responsible Officer
SRP	Service Reporting Period
SSP	Self Service Portal
SSS	Specialist Security Services
STCF	Supplier Test Collaboration Forum
STF	SIAM Transition Function
SyOPs	Security Operating Procedures
TCO	Total Cost of Ownership

TCP	Transmission Control Protocol
TDA	Technical Design Authority
TMMi	Test Maturity Model integration
TMO	Transition Mode of Operations
TO	Technical Observation
TOC	Transition Operational Control
TOGAF	The Open Group Architecture Framework
TOI	Transfer of Information
TOM	Target Operating Model
TOR	Terms Of Reference
TSA	Tower Service Agreement
TSDM	Testing Service Delivery Manager
UAT	User Acceptance Testing
UC	Underpinning Contract
UDP	User Datagram Protocol
UK	the United Kingdom
UKAS	The United Kingdom Accreditation Service
UPS	Uninterrupted Power Supply
UTC	Coordinated Universal Time
VAT	Value Added Tax
VBF	Vital business functions
VFM	Value for Money
VLAN	Virtual Local Area Networks
VOI	Value On Investment
VoIP	Voice over Internet Protocol
VVI	Voice Video Network Integration
WAN	Wide Area Network
WBS	Work Breakdown Structure
WIP	Work In Progress – Projects, Programmes and BAU changes

2. DEFINITIONS

- 2.1 In this Agreement, unless the context otherwise requires:
- 2.1.1 expressions listed in this paragraph 2 shall have the meanings set out below;
 - 2.1.2 the expressions listed in ITIL shall have the meanings given to them in ITIL;
 - 2.1.3 the expressions listed in CESG Good Practice Guide 13 shall have the meanings given to them in CESG Good Practice Guide 13;
 - 2.1.4 the expressions listed in CESG Good Practice Guide 18 shall have the meanings given to them in CESG Good Practice Guide 18; and
 - 2.1.5 the expressions listed in schedule 9.1 (Staff Transfer) shall have the meanings given to them in schedule 9.1 (Staff Transfer).
- 2.2 If there is any conflict between the meaning given to an expression in ITIL and the meaning given to the expression in this schedule 1 (Definitions), then the meaning given to that expression in this schedule 1 (Definitions) shall apply.
- 2.3 Paragraph 2.1.2 shall apply to ITIL expressions that may be used in this Agreement with a capital first letter, but which are listed in ITIL with a lower-case first letter.
- 2.4 This Agreement also contains capitalised references to names of some of the following items, which may not be listed in this schedule 1 (Definitions):
- 2.4.1 Referenced Documents, which are described further in schedule 11 (Referenced Documents);
 - 2.4.2 Documentary Deliverables, further detail on which may be available in the relevant Product Descriptions associated with such Documentary Deliverables;
 - 2.4.3 Service Requirements, which are described further in schedule 2.1 (Service Requirements); and
 - 2.4.4 governance Boards, which are described further in schedule 8.1 (Governance).

Term	Definition
“2020 Hosting Agreement”	has the meaning given in paragraph a of the Introduction to this Agreement;
“Acceptance Criteria”	the criteria for Approval of a Milestone or other element of a FITS Service as outlined in Appendix B to schedule 6.1 and established and developed in accordance with clause 5 (Milestones, Testing and Approval) and schedule 6.1 (including any criteria set out in the Project Notification relating to that Milestone or FITS Service);
“Account Test Manager”	has the meaning given to it in the Authority Test Strategy;

Term	Definition
“Accounting”	has the meaning set out in paragraph 36 of the standard GPG13 - Good Practice Guide Protective Monitoring for HMG ICT Systems, October 2012, Issue No: 1.7;
“Accounting Items”	has the meaning set out in paragraph 48 of the standard GPG13 - Good Practice Guide Protective Monitoring for HMG ICT Systems, October 2012, Issue No: 1.7;
“Accounting Reference Date”	means the dates to which the Hosting Supplier prepares its audited financial statements;
“Accreditation”	a formal, independent assessment of an End To End ICT Environment or End To End Service against the Information Security Management service requirements set out in schedule 2.1 (Service Requirements) or such other requests as may be notified to the Hosting Supplier from time to time, and “Accredited” shall be construed accordingly;
“Accreditation Lead”	the lead certifier for ICT services that require accreditation;
“Accreditor”	the person or body engaged to carry out an Accreditation;
“Achieve”	in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the applicable acceptance procedure for that Milestone where the associated Acceptance Criteria have been met. “Achieved” and “Achievement” shall be construed accordingly;
“ACPO 'Good Practice Guide for Computer-Based Electronic Evidence’”	describes the best practice guidelines and approaches required for digital forensic investigations on computer-based electronic evidence. See http://www.7safe.com/electronic_evidence/ ;
“Active User”	the number of unique End User logons executed (excluding Hosting Supplier Personnel) within the directory service as a subset of the available logins, from the 16th calendar day of the previous Service Reporting Period to the 15th calendar day of the current Service Reporting Period;
“Affected Party”	the party seeking to claim relief in respect of a Force Majeure Event;
“Affiliate”	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
“Agreement”	the clauses of this Agreement together with the schedules, Appendices and annexes to it and any documents referred to or attached to it;
“AMS Services”	the services provided by the AMS Suppliers;
“AMS Supplier” or “Application Maintenance Support Supplier”	a supplier under an agreement between the Authority and a provider of applications maintenance and support services under the FITS Programme;
“Application”	ICT services which enable the Authority to discharge its obligations and business function;

Term	Definition
“Application Directory”	the store of user identity attributes, credentials and user role information for one or more Business Applications;
“Application of Revised Service Charges”	the application of revised service charges Bounded Mechanism as further described in paragraph 7.12 of schedule 7.1 (Charging and Invoicing);
“Application Performance Baseline”	a measure of the performance of a FITS Service or a Business Application at a point in time which is used as a baseline against which future performance shall be assessed;
“Approval”	means, in respect of a Deliverable, a Milestone, an element of the FITS Service or a Documentary Deliverable, to successfully meet its Acceptance Criteria, Quality Criteria (as applicable) and have the appropriate Approval Certificate issued, and “Approve” and “Approved” shall be construed accordingly;
“Approval Certificate”	a certificate supplied by the Authority when a Deliverable meets all its Approval Criteria;
“Approval Criteria”	in respect of a Milestone, or a FITS Service means its Acceptance Criteria, and in respect of a Documentary Deliverable means its Quality Criteria;
“Approval Failure”	where a review of a Documentary Deliverable is recorded as unsuccessful because the relevant Quality Criteria have not been met;
“Approval Procedure”	the processes and procedures set out in schedule 8.7 (Document Approval Procedure);
“Approval Success”	shall have the meaning given to it in clause 5.11;
“Architectural Board”	the governance board with the same title as specified in Schedule 3 (Governance) of the MSA;
“Architecture”	the structure of a system or FITS Service, including the relationships of components to each other and to the environment they are in;
“Architecture Artefact”	Documentation, such as high level or low level designs, that describes an aspect of the Architecture and supports the delivery, management, or maintenance of FITS Services;
“Architecture Management”	a process for supporting the alignment of IS/IT provision to business needs - by defining, describing, modelling, mapping, and communicating the relationships between the as-is and to-be business requirements, business functions, IS/IT systems and services, their component parts and the environment they are in. Architecture management includes the creation and consolidation of data, documents and models pertaining to the different domains or scopes - including the Authority as a whole (Enterprise Architecture); the implementation of specific real-world solutions (solution architecture) and the operation of all real world components to provide the Authority with End to End Services (Deployed Architecture). Architecture management includes management of the Standards and guidelines that guide the design,

Term	Definition
	evolution and operation of the solutions; and includes governance processes integrated with change and ICT planning and delivery lifecycles to ensure alignment with the to-be landscape;
“Arms-length Body”	a body or office listed in the Public Bodies Act 2011;
“Asset Management”	an activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle;
“Asset Management System”	a system developed for the management of assets and asset information;
“Assets”	all assets and rights used by the Hosting Supplier to provide the Hosting and/or FITS Services in accordance with this Agreement and any reference to such assets as they may be changed, replaced, modified, updated or subject to any programmed replacement of lifecycle regime from time to time, but excluding the Authority Assets;
“Assistive Technology”	assistive, adaptive, and rehabilitative software and hardware for people with disabilities and also includes the process used in selecting, locating, and using them. Assistive Technology (AT) is designed to enable independence for disabled people;
“Assurance Report”	a report documenting the findings, conclusions and recommendations following the completion of an activity or Deliverable to the requirements;
“ATP Milestone”	any Milestone where a Milestone Achievement Certificate is required before a FITS Supplier can proceed with further activities or commence delivery of further FITS Services and/or Cross Tower Services;
“ATP Milestone Date”	the due date for Achievement of any ATP Milestone as set out in the the Transition Table;
“Audio Conference Service”	a service to allow multiple End Users and multiple external callers to participate in audio conferencing calls using designated Authority accounts and personal identification numbers to gain access to the service;
“Audit Rights”	permissions to perform controlled and defined checks on a prescribed aspect of business and / or ICT process and data, against a defined set of criteria;
“Authentication”	the assurance that a person or device is the legitimate owner and user of the asserted identity;
“Authorised Representative”	an individual that has been authorised by the Authority to act and decide on its behalf during certain activities;
“Authorised Users”	users authorised to access ICT services or data or to grant other Users such authorisation;
“Authority Assets”	the Authority Materials, the specially written material, the authority infrastructure and any other data, software, assets, equipment or other property owned by the Authority and which is

Term	Definition
	or may be used in connection with the provision or receipt of the Hosting and/or FITS Services, including the Hardware Assets;
“Authority Cause”	any breach by the Authority of any of the Authority’s Responsibilities except to the extent that it is the result of any act or omission by the Authority to which the Hosting Supplier has given its prior consent;
“Authority Confidential Information”	all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Authority, including all IPR, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked “confidential”) or which ought reasonably be considered to be confidential;
“Authority Data”	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: <ul style="list-style-type: none"> (a) supplied to the Hosting Supplier by or on behalf of the Authority or which the Hosting Supplier is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Data Controller;
“Authority Materials”	the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority to the Hosting Supplier, the IPR in which: <ul style="list-style-type: none"> (a) are owned or used by or on behalf of the Authority; and (b) are or may be used in connection with the provision or receipt of the Hosting and/or FITS Services, but excluding any specially written material, Hosting Supplier Material and Third Party Material;
“Authority Personnel”	all employees, agents, consultants and contractors of the Authority;
“Authority Project Manager”	the representative from the Authority who is responsible for the relevant Project;
“Authority Provided Services”	any part of the End to End Services provided by the Authority;
“Authority Representative”	the representative appointed by the Authority pursuant to clause 23.1 (Representatives);
“Authority SI Function”	the part of the System Integration function that will be delivered by the Authority;
“Authority Site”	Sites owned, controlled or occupied by the Authority and Other Authority Providers which are made available or used by the Hosting Supplier or its Sub-contractors for provision of the Hosting and/or FITS Services (or any of them) on the terms set

Term	Definition
	out in this Agreement or any separate agreement or licence;
“Authority Software”	software which is owned by or licensed to the Authority, including software which is or will be used by the Hosting Supplier for the purposes of providing the Hosting Services and/or FITS Services but excluding the Hosting Supplier Software;
“Authority Test Assurance”	the Test Assurance activities conducted by the Authority;
“Authority Test Strategy”	the document referred to as such in schedule 11 (Reference Documents);
“Authority to Proceed”	agreement by the Authority for a FITS Supplier to commence certain activities and/or commence delivering any FITS Services and/or Cross Tower Services that are identified in the Transition Portfolio Plan, the Transition Plan or a Project Plan as requiring such agreement;
“Authority's Change Manager”	the person appointed to that position by the Authority from time to time and notified in writing to the Hosting Supplier or, if no person is notified, the Authority Representative;
“Authority's ICT Environment”	an ICT Environment owned by the Authority;
“Authority's ICT Integrated Lifecycle”	the Authority's ICT process framework used to progress business demand from request to delivery and closure. It identifies the main processes, deliverables and quality gates. Often referred to as the Authority's ICT Integrated Lifecycle;
“Authority's Responsibilities”	the responsibilities of the Authority specified in schedule 3.1 (Authority Responsibilities);
“Authority's Strategic ICT Objectives”	the Strategic objectives listed and described in the Authority's ICT strategy;
“Availability” or “Available”	has the same meaning as “Service Availability” ;
“Availability Management Information System”	a set of tools, data and information that is used to support availability management;
“Average Price”	in relation to the Comparable Services provided by the Comparison Group, the mean average of prices for those Comparable Services as adjusted to produce Equivalent Services Data over the previous twelve (12) month period, or other period as agreed between the Authority and the Hosting Supplier. (For the avoidance of doubt, the “mean average price” shall be calculated by aggregating the prices derived from Equivalent Services Data for each of the services and dividing the same by the number instances of Comparable Services);
“Back out Plan”	a plan for reverting to the pre-change configuration of a FITS Service following the failed implementation of a change into the live environment;
“Base Application”	a Business Application denoted as such within the Master

Term	Definition
	Application List, but typically with the following characteristics: a Business Application for which a degradation or loss of the service would impact on the productivity of an individual End User or a small number of End Users;
“Base Case Financial Model”	the financial model projecting Costs and Charges in relation to the provision of Hosting and/or FITS Services prepared by the Hosting Supplier as at the Effective Date consistent with the requirements in schedule 7.5 (Financial Model);
“Base Cost”	the direct cost to the Hosting Supplier, calculated per Person Day, of employing the Hosting Supplier Personnel, expressed per individual, and including (without limitation): <ul style="list-style-type: none"> salary cost; staff training; work place accommodation; ICT equipment and tools; pension allowances; car allowances; and any other fringe benefits;
“Board”	a formal Governance committee whose roles and responsibilities are outlined in schedule 8.1 (Governance);
“Board Confirmation”	means the written confirmation from the Supplier Board in accordance with paragraph 10 of schedule 7.4 (Financial Distress);
“Boundary Gateway”	a Boundary Gateway is used to demarcate the edge of an ICT Environment provided by a Supplier within the FITS ICT Environment and where necessary, implement security controls to protect Information Assets held within and transferred between ICT Environments. These gateways may be implemented to ensure the scope for Accreditation is clearly defined;
“Bounded Mechanism”	a mechanism agreed by the parties in accordance with paragraph 7 of schedule 7.1 (Charging & Invoicing);
“Breach of Security”	the occurrence of: <ul style="list-style-type: none"> (a) any unauthorised access to or use of the Hosting Services, the Authority Sites, and/or any End to End ICT Environment, information or data (including the Confidential Information and the Authority Data) used by the Authority and/or the Hosting Supplier in connection with this Agreement; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Hosting Supplier in connection with this Agreement;

Term	Definition
“Breakage Costs”	any costs (such as the Hosting Supplier's own redundancy costs, and costs payable for early termination of contracts entered into by the Hosting Supplier prior to receipt of the Termination Notice) incurred by the Hosting Supplier directly as a result of the termination of this Agreement which: <ul style="list-style-type: none"> (a) would not have been incurred had this Agreement continued until its natural expiry; (b) relate directly to the termination of the Hosting Services; (c) are unavoidable, proven, reasonable, and not capable of recovery; (d) are incurred under arrangements or agreements that are consistent with the terms of this Agreement and on reasonable commercial terms; and (e) do not relate to contracts or subcontracts with Affiliates of the Hosting Supplier;
“Business Application”	the applications listed in Appendix 6 of Schedule 4.1 ((Hosting Supplier Solution) as amended from time to time in accordance with the Change Control Procedure;
“Business As Usual”	the routine activities performed by the Authority's Business Units;
“Business As Usual Governance”	any governance forum not associated with the End to End Transition activities, as detailed in schedule 8.1 (Governance) and the MSA;
“Business Continuity”	the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level;
“Business Continuity and Disaster Recovery Plan”	any plan prepared pursuant to schedule 8.6 (Business Continuity), as may be amended from time to time;
“Business Impact Assessment”	an assessment resulting in an associated report outlining the risks to the Information Assets;
“Business Impact Level”	a measurement of the impact resulting from a compromise of confidentiality, integrity and availability of an ICT Environment, in accordance with HMG Security Policy Framework;
“Business Process Manual”	a manual setting out a detailed definition of all the business processes that shall be supported by the Hosting Services;
“Business Record Management (Processes)”	the practice of maintaining the records of an organisation from the time they are created up to their eventual disposal;
“Business Units”	a logical element or segment of the Authority carrying out a set of distinct functions and services including but not limited to the Authority's HQ, NOMS, HMCTS, A2J, LSC, and ALBs;

Term	Definition
“C.O. Statement”	the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector;
“Call Barge”	the capability that allows a Key User to interrupt a call that is in progress;
“Capacity Management Information System”	a set of tools, data and information that is used to support capacity management;
“Capacity Plan”	the plan described in schedule 2.1 (Service Requirements) that is produced to ensure that the Hosting Supplier ICT Environment and the Hosting Services delivered by the Hosting Supplier will have sufficient capacity to cope with all known contingencies and with planned expansion or contraction of the Hosting Services;
“Capital Costs”	those costs which would be treated as capital costs according to generally accepted accounting principles within the UK which shall include the cost to be charged in respect of Assets by the Hosting Supplier to the Authority or (to the extent that risk and title in any Asset is not held by the Hosting Supplier) any cost actually incurred by the Hosting Supplier in respect of those Assets;
“Carbon Reduction Plan”	the Hosting Supplier's carbon reduction plan maintained in accordance with paragraph 4 of annex 1 (Sustainability and Social Value Requirements) of Schedule 2.1 (Service Requirements);
“Card Holder Data Environment”	Devices and Software which the appointed Payment Card Industry (PCI) Qualified Security Assessor (QSA) has specified are within the scope of the Card Holder Data Environment;
“Case Summary”	a concise summary of a party's case in a Dispute subjected to mediation;
“CEDR”	the Centre for Effective Dispute Resolution of International Dispute Resolution Centre, 70 Fleet Street, London, EC4Y 1EU;
“Central Government Body”	a body listed in one of the following sub-categories of the Central Government Classification of the Public Sector Classification Guide, as published and amended from time to time by the Office of National Statistics: <ul style="list-style-type: none"> (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive or tribunal); (c) Non-Ministerial Department; or Executive Agency;
“Certificate of Costs” or “Certification of Costs”	a certificate of costs provided by the Hosting Supplier in accordance with paragraph 11 of schedule 7.1 (Charging & Invoicing);
“Change”	any Contract Change or Operational Change;
“Change Communication”	any Change Request, Impact Assessment, Change Authorisation Note or other communication sent or required to be sent pursuant to schedule 8.2 (Change Control Procedure);

Term	Definition
“Change Control Procedure”	the procedure for changing this Agreement, as set out in schedule 8.2 (Change Control Procedure);
“Change in Law”	any change in Law, which impacts on the performance of the Hosting Services which comes into force after the Effective Date;
“Change Management”	the change management procedure defined by the SIAM Supplier pursuant to the Change and Evaluation Management requirements set out in schedule 2.1 (Service Requirements);
“Change of Control”	a change in Control of the Hosting Supplier or a Key Sub-contractor;
“Change Request Part A: Initial Request”	a written or electronic request for a Contract Change which shall be substantially in the form of Appendix 1 to schedule 8.2 (Change Control Procedure);
“Change Request Part B1: Technical and Business Impact Assessment”	a written or electronic technical assessment of the impact that a Change Request would make on the Agreement, which shall substantially contain the information shown in Part B1 of Appendix 1 of schedule 8.2 (Change Control Procedure);
“Change Request Part B2: Financial Impact Assessment”	a written or electronic assessment of the resources and costs required to complete a Change Request, which shall substantially contain the information shown in Part B2 Appendix 1 of schedule 8.2 (Change Control Procedure);
“Change Request Part C: Change Authorisation”	the form used by the parties to set out the agreed Contract Change and which shall be substantially in the form of Appendix 1 to schedule 8.2 (Change Control Procedure);
“Charges”	the charges for the provision of the services set out in and derived in accordance with schedule 7.1 (Charging and Invoicing), including any Milestone Payment, Stage Payment or Service Charge;
“CHECK”	a CESG operated scheme that provides CESG accredited companies that employ CHECK accredited penetration testers qualified to assess HMG systems up to CONFIDENTIAL, and including SECRET with CESG approval;
“CHECK Report”	a report detailing the findings of a CHECK Test;
“CHECK Resolution Plan”	a detailed proposal which describes the activities and resources needed and timescales to mitigate the findings listed in the CHECK Report;
“CHECK Scope”	a document developed by the IT Health Check Supplier based on the Approved CHECK Test Statement of Requirements produced collaboratively by the Other FITS Suppliers;
“CHECK Team Leader”	an individual employed by a CHECK approved company who has passed the requisite CHECK Team Leader exam and has been designated by CESG as a CHECK Team Leader;
“CHECK Team Member”	an individual employed by a CHECK approved company who has achieved the requisite CHECK Member entrance requirements and has been designated by CESG as a CHECK Team Member;

Term	Definition
“CHECK Test” or “CHECK Testing”	the Test or Testing carried out by the IT Health Check Supplier;
“CHECK Test Statement of Requirements”	a document produced collaboratively by the Suppliers to define the CHECK Test requirements. It is used as the benchmark for producing the CHECK Scope document;
“CHECK Testing Roadmap”	a document produced by the Authority to provide detail of when CHECK Testing will take place across the Authority ICT Environments;
“CHECK Testing Strategy”	a document produced by the Authority to provide guidance and the approach to CHECK Testing within the Authority;
“Client Builds”	an approved, and tested package of Client Software which allows the Client Device to function in a standard manner;
“Client Device”	the hardware utilised by an End User to receive End to End Services, including, but not limited to desktops, Mobile Client Devices, thin client devices and kiosks;
“Client Device Video Services”	a peer-to-peer video and image sharing service that enables End Users to exchange multimedia content with one or multiple contacts simultaneously in a multiplex and real-time manner via Client Devices;
“Client Software”	the Software executed or presented on a Client Device and used to access End to End Services;
“CMO Services”	services provided by Exiting Suppliers or Other Authority Providers;
“Collaborating Supplier”	has the meaning given to it in schedule 8 (Definitions & Interpretation) of the Master Services Agreement;
“Collaborating Supplier ICT Environment”	an ICT Environment used by a Collaborating Supplier to provide a service under a Supply Agreement;
“Commercial Contract Management Board”	means the board more particularly described in paragraph 2.6 of schedule 8.1 (Governance);
“Commercial Off the Shelf Software”	mass produced commercially available Software used in the provision of the FITS Services;
“Commercially Sensitive Information”	the information listed in schedule 4.2 (Commercially Sensitive Information) comprising the information of a commercially sensitive nature relating to the Hosting Supplier, its IPR or its business or which the Hosting Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Hosting Supplier significant commercial disadvantage or material financial loss;
“Communications-Electronics Security Group”	UK Government's National Technical Authority for Information Assurance;
“Comparable Supply”	the supply of services to another customer of the Hosting Supplier that are the same or similar to the Hosting and/or FITS Services;

Term	Definition
“Compensation Payment”	a payment to compensate for a loss of profit;
“Confidential Information”	the Authority Confidential Information and/or the Hosting Supplier's Confidential Information;
“Configuration Item”	any component that needs to be managed in order to deliver a FITS Service and which may include IT services, hardware, software, buildings, people and formal documentation such as process documentation and agreed levels of service;
“Configuration Management System”	a Configuration Management System is a set of tools, data and information that is used to support Service Asset and Configuration Management. The CMS includes tools for collecting, storing, managing, updating, analysing and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes and releases;
“Connection”	a logical or physical connection between the FITS ICT Environments and an external network (see also “Connection Criteria”);
“Connection Criteria”	a mandatory set of requirements the Achievement of which must be demonstrated before connecting to a given network, as set out in schedule 2.1 (Service Requirements);
“Consolidated Asset Register”	the consolidation of the various Asset Registers to be maintained by the SIAM Supplier;
“Consolidated Test Schedule”	the consolidated schedule (timings and dependencies) of all Testing activities across all FITS Towers during the End to End Transition Period, produced and managed by FTAF, as set out in schedule 6.1 (Project Management);
“Content Management Application” (CMA)	the front end component of a content management system; the CMA interface allows users to create and manage corporate or website content;
“Contract Change”	any change to this Agreement other than Operational Change;
“Contract Compliance”	as set out in paragraph 9.3.1 of schedule 6.1 (Project Management);
“Contract Performance Point”	the point in time after a SCD when a FITS Supplier successfully demonstrates to the Authority that a FITS Service and/or Cross Tower Service is working satisfactorily in the Live Environment which is anticipated to be linked to the Project Milestone which is referred to as the “CPP Milestone” in the Transition Table;
“Contract Year”	<p>(a) a period of twelve (12) months commencing on the Effective Date; or</p> <p>(b) thereafter a period of 12 months commencing on an anniversary of the Effective Date</p> <p>provided that the final Contract Year shall end on the expiry or termination of the Term;</p>

Term	Definition
“Contracts Finder”	the Government’s publishing portal for public sector procurement opportunities;
“Contracting Authority”	any contracting authority as defined in Regulation 2 of the Public Contracts Regulations 2015 other than the Authority;
“Control”	that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Conviction”	other than for minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding-over orders (including any spent convictions as contemplated by section 1(1) of the Rehabilitation of Offenders Act 1974 by virtue of the exemptions specified in Part II of schedule 1 of the Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975 (SI 1975/1023), or any replacement or amendment to that Order, or being placed on a list kept pursuant to section 2 of the Safeguarding Vulnerable Groups Act 2006;
“Correction Plan”	the Hosting Supplier's plan for the remediation of any test issues or the resolution of any non-conformities in any Deliverable to be agreed in accordance with clause 6 (Delays - General Provisions);
“Cost Model”	a framework used in budgeting and accounting in which all known costs can be recorded, categorized and allocated to specific Business Units or projects;
“Costs”	the costs to be incurred by the Hosting Supplier in providing the Hosting and/or FITS Services including the Base Cost and the Overhead;
“CPP Milestone”	any Milestone where CPP is required before a FITS Supplier can recover any Forecast Profit relating to such Milestone, as detailed in schedule 7.1 (Charging and Invoicing);
“CPP Milestone Date”	the due date for Achievement of any CPP Milestone as set out in the Transition Table;
“Credit Rating Thresholds”	the credit rating thresholds as set out in Appendix 2 to schedule 7.4 (Financial Distress);
“Critical Incident”	an unanticipated occurrence that causes destruction, loss, or distress to the Hosting Supplier, including natural disasters, technological accidents, or human-caused events, that may result in significant asset loss or damage, multiple injuries or death;
“Cross Tower Services”	has the meaning given to it in schedule 8 (Definitions) of the Master Services Agreement;
“Crown”	the government of the United Kingdom (including the Northern Ireland Executive Committee and Northern Ireland Departments, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers, government departments and particular bodies, persons and government

Term	Definition
	agencies;
“Crown Body”	any department, office or agency of the Crown;
“Cutover(s)”	the implementation of the activities performed to affect the transition of responsibilities for the delivery of a service from a party to a FITS Supplier;
“Cutover Plans”	a plan for the activities to be undertaken during the cutover of a FITS Service;
“Data Centre Facility”	Site(s) owned, controlled or occupied by a Data Centre Supplier, other than the REDACTED Data Centre Facility, which are used for the delivery by a Data Centre Supplier or its Sub-contractors for the provision of Data Centre Services; Sites owned, controlled or occupied by the Data Centre Supplier which are used for the delivery by the Data Centre Supplier or its Sub-contractors for the provision of Data Centre Services.
“Data Centre Services”	the services provided by the Data Centre Supplier;
“Data Centre Supplier”	Site(s) owned, controlled or occupied by a Data Centre Supplier, other than the REDACTED Data Centre Facility, which are used for the delivery by a Data Centre Supplier or its Sub-contractors for the provision of Data Centre Services; a supplier under an agreement between the Authority and a provider of data centre services under the FITS Programme;
“Data Controller”	shall have the same meaning as set out in the Data Protection Legislation;
“Data Loss Event”	any event which results, or may result, in unauthorised or unlawful Processing of Authority Personal Data held by the Supplier under the Agreement, and/or actual or potential loss and/or destruction of and/or damage to Authority Personal Data in breach of the Agreement, including any Personal Data Breach;
“Data Processor”	shall have the same meaning as set out in the Data Protection Legislation;
“Data Protection Impact Assessment”	an assessment carried out pursuant to Article 35 of the UK GDPR;
“Data Protection Legislation”	the Data Protection Act 2018, for so long as it is applicable under English law, the European Regulation 2016/679 relating to the processing of Personal Data as of its date of application (“ GDPR ”) and any implementing laws of the GDPR to which the Data Controller is subject, the UK GDPR, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice

Term	Definition
	issued by the Information Commissioner;
“Data Protection Requirements”	the requirements under the Data Protection Legislation;
“Data Subject”	shall have the same meaning as set out in the Data Protection Legislation;
“Database”	the rights in or to the database developed and supplied by the Hosting Supplier to the Authority in accordance with the terms of this Agreement;
“Default”	any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub-contractors in connection with or in relation to the subject-matter of this Agreement or the Master Services Agreement and in respect of which such party is liable to the other;
“Deferred Shareholder Fund”	has the meaning given to in schedule 8 (Definitions) of the Master Services Agreement;
“Delay”	the period of time by which the implementation of the Hosting and/or FITS Services is delayed arising from a failure to Achieve a Milestone;
“Delay Payments”	the amounts payable by the Hosting Supplier to the Authority in respect of a Delay and specified in schedule 7.1 (Charging and Invoicing);
“Deliverable”	an item, feature, document or service associated with the provision of the FITS Services or a change in the provision of the FITS Services which is required to be delivered by the Hosting Supplier at any stage during the performance of this Agreement, including at any Milestone;
“Delivery Dependencies”	the Dependencies identified by the Hosting Supplier in the Hosting Supplier Solution relevant to Transition and as set out in the Delivery Dependencies Log;
“Delivery Dependencies Log”	the document setting out all the Dependencies during Transition. As at the Effective Date the Delivery Dependencies Log is included at schedule 4 to the MSA which is populated with the Delivery Dependencies from the Hosting Supplier’s Solution, the Transition Table, the equivalents from Other FITS Suppliers as well as Delivery Dependencies Approved in Projects that are live as at the Effective Date. Thereafter the Delivery Dependencies Log will be deemed to be amended and updated each time a Project Authority to Proceed is issued or a Dependency has been met;
“Dependencies Register”	has the meaning given to it in the Master Services Agreement;
“Dependency”	has the meaning given to it in the Master Services Agreement;
“Deployed Architecture”	data, documents and models pertaining to and describing the operation of all real world components that provide the Authority

Term	Definition
	with End to End Services;
“Deposited Software”	the Software the Source Code of which is to be placed in escrow as listed in paragraph 5 of schedule 5.1 (Software);
“Designated Space”	the space and premises made available from time to time by the Data Centre Supplier and in respect of which a licence to occupy is granted pursuant to clause A69 (Licence to use Designated Space);
“Destruction Certificate”	certifies that protectively marked or classified information or physical assets have been disposed of in line with Information Assurance Standard No.5;
“Detailed Transition Deliverables”	an item, document, feature or service associated with the provision of the FITS Services or a change in the provision of the FITS Services which is required to be delivered by a FITS Supplier at a Milestone Date or at any other stage during in the performance of this Agreement and which is described in the Final Transition Portfolio Plans as a “Deliverable”;
“Device”	any physical hardware used in the delivery of FITS Services;
“Dial Plan”	the numbering schema used in telecommunications to allocate telephone ranges to regions, areas and sites. The Dial Plan defines the rules for assigning numbers to Devices to ensure there is a consistent and logical relationship across the End to End ICT Environment and external networks such as the PSTN. The Dial Plan shall comply with PSN standards and formats to enable cross-PSN dialling and any number translation required when connecting private voice networks to the PSTN;
“Digital Forensic Investigation”	any test or live investigation involving Digital Evidence and exercise of Forensic Readiness Plans;
“Digital Forensic Investigators”	professionals who conduct Digital Forensic Investigations;
“Digital Forensics Readiness Policy”	the Forensic Readiness Policy within the SKL;
“Digital Forensic Report”	a report detailing the findings of a Digital Forensic Investigation;
“Digital Forensic Resolution Plan”	a detailed proposal which describes the activities and resources needed and timescales to mitigate the findings listed in the Digital Forensic Report;
“Digital Forensics Services”	the services provided by the Digital Forensics Supplier(s);
“Digital Forensics Supplier”	a supplier under an agreement with the Authority for the provision of computer forensic or Digital Forensic Services;
“Directory Services”	has the meaning given to it in the Service Register;
“Disaster”	the occurrence of one or more events which, either separately or cumulatively, mean that the Hosting Services and/or the Cross Tower Services, or a material part of them will be unavailable for

Term	Definition
	a period or which is reasonably anticipated will mean that the Hosting Services and/or the Cross Tower Services, or a material part of them will be unavailable for that period;
“Disaster Recovery”	the process of restoration of the Hosting Services by the provision of the Disaster Recovery Plan;
“Disaster Recovery Plan” or “DR Plan”	the plan described in paragraph 5 of Part C of schedule 8.6 (Business Continuity);
“Disaster Recovery Services”	the disaster recovery and/or business/service continuity services (as the context may require) to be provided by the Network Supplier pursuant to schedule 6.5 (BCDR Provisions) of the Networks Supplier TSA;
“Disaster Recovery System”	the system identified by the Network Supplier in the Network Supplier's Solution which shall be used for the purpose of delivering the Disaster Recovery Service;
“Dispute”	any dispute, difference or question of interpretation arising out of or in connection with this Agreement, including any dispute, difference or question of interpretation relating to the Hosting and/or FITS Services, failure to agree in accordance with the Change Control Procedure or any matter where this Agreement directs the parties to resolve an issue by reference to the Dispute Resolution Procedure;
“Dispute Resolution Procedure”	the dispute resolution procedure set out in schedule 8.3 (Dispute Resolution Procedure);
“Document Approval Procedure”	the procedures for review and Approval of Documentary Deliverables as set out in schedule 8.7 (Document Approval Procedure);
“Document Review Plan”	a plan for undertaking the review and Approval of a Documentary Deliverable, as described in paragraph 4.2 of schedule 8.7 (Document Approval Procedure);
“Documentary Deliverables”	deliverables that take the form of Documentation;
“Documentation”	the descriptions of the Hosting Services and/or FITS Services and Service Levels, technical specifications, user manuals, operating manuals, process definitions and procedures, and all such other documentation as: <ul style="list-style-type: none"> (a) is required to be supplied by the Hosting Supplier to the Authority under this Agreement; (b) is required by the Hosting Supplier in order to provide the Hosting Services and/or FITS Services; or (c) has been or shall be generated for the purpose of providing the Hosting Services and/or FITS Services;
“DOTAS”	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within

Term	Definition
	set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992;
“DP Process” and “DP Processing”	has the meaning given to "process" under the Data Protection Legislation but, for the purposes of this Agreement, it shall include both manual and automatic processing;
“Earned Expenses”	all amounts recognised as costs in accordance with generally accepted accounting principles within the United Kingdom but excluding taxation, funding and similar costs, amounts payable under paragraph 13 of schedule 7.1 (Charging & Invoicing), capital expenditures and non-cash items (including but not limited to depreciation, amortisation, impairments and movements in provisions) incurred by the Hosting Supplier in each Contract Year;
“Earned Gain”	Earned Revenue less Earned Expenses, divided by Earned Revenue and expressed as a percentage;
“Earned Revenue”	all Charges paid or payable to the Hosting Supplier by the Authority under this Agreement in each Contract Year;
“Effective Date”	the date on which this Agreement is signed by both parties;
“Embedded Third Party IPR”	any Third Party Software which is embedded in or which is an integral part of the Specially Written Software or Database (as applicable) together with any Third Party Materials related to that Third Party Software;
“Emergency Exit”	any termination of this Agreement which is a (i) termination of the whole or part of this Agreement in accordance with clause 57 (Termination Rights), except where the period of notice given under that clause is greater than or equal to six months; (ii) termination of the provision of the Hosting Services for any reason prior to the expiry of any period of notice of termination served pursuant to clause 57; or (iii) wrongful termination or repudiation of this Agreement by either party;
“Employee Liabilities”	all claims, including claims for redundancy payments, unlawful deduction of wages, unfair, wrongful or constructive dismissal compensation, compensation for sex, race or disability discrimination, claims for equal pay, compensation for less favourable treatment of part-time workers, and any claims (whether in tort, contract or statute or otherwise), demands, actions, proceedings and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs and expenses reasonably incurred in connection with a claim or investigation (including any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of

Term	Definition
	implementing any requirements which may arise from such investigation), and any legal costs and expenses;
“Employment Regulations”	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the Council Directive 77/187/EEC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses;
“Enabling Authority Business Transformation”	where used, has the meaning given to it in paragraph 4.1.1 of schedule 2.4 (Transformation);
“End of Life” or “EoL”	in relation to the Hosting Supplier ICT Environment where: <ul style="list-style-type: none"> (a) the manufacturer no longer sells that model of hardware; (b) the manufacturer no longer offers supports for that model of hardware, in particular the manufacturer no longer provides software updates, including security and vulnerability patches; and/or (c) the manufacturer will only offer support for that model of hardware conditional on specified actions being undertaken by the Authority (or by the Hosting Supplier on the Authority's behalf), and the Authority will not agree to such actions and as a result the support cannot be obtained);
“End to End ICT Environment”	the Authority's ICT Environment, the FITS Supplier ICT Environments, the Collaborating Supplier ICT Environments, the Exiting Supplier ICT Environments and the Other Authority Provider ICT Environments providing End to End Services or components thereof;
“End to End Services”	all FITS Services and all other ICT services supplied to the Authority;
“End to End Transition”	the period from the effective date of the SIAM Supplier's Tower Service Agreement (i.e. 3 rd September 2013) to Grand FMO;
“End User”	any user authorised to use and/or access End to End Services or data including but not limited to: Authority Personnel; the Judiciary; Crown Bodies personnel; Arms-length Bodies' personnel, Suppliers' personnel; Other Authority Providers' personnel and the Authority's customers;
“Enhanced Application”	a Business Application denoted as such within the Master Application List, but typically with the following characteristics: a Business Application for which a degradation or loss of the service would have a significant impact on the Authority's productivity and / or reputation;
“Enhanced Licence Terms”	the licence terms set out in Part B (Enhanced Licence Terms) of schedule 5.2 (Licence Terms);

Term	Definition
“Enterprise Architecture”	a process for supporting the translation of business vision and strategy into effective enterprise change - by defining, describing, modelling, mapping and communicating the as-is and to-be business requirements, business functions, IS/IT systems and services; and developing and describing the roadmaps and strategies for moving from the as-is to the to-be state, at the generalised, enterprise level;
“Environmental Information Regulations”	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government department in relation to such regulations;
“EoL Media Communication Plan”	the plan setting out how the parties will liaise with each other regarding any press announcements that the Authority may make in respect of any Service Failure which is as a result of the Hosting Supplier ICT Environment being at End of Life, to be agreed in accordance with clause 54.11;
“Escalation Process”	the initial stages of the process for dealing with Disputes without the intervention of third parties as set out in paragraph 2 of schedule 8.3 (Dispute Resolution Procedure);
“Escrow Agent”	the agent appointed by the Authority to hold the Deposited Software, pursuant to schedule 5.3 (Escrow Terms);
“Escrow Agreement”	the agreement entered into between the Authority, the Hosting Supplier and the Escrow Agent, pursuant to schedule 5.3 (Escrow Terms);
“Estates Management Matrix”	as set out in paragraph 5.11.2 of schedule 6.1 (Project Management);
“EUCS Services”	the services provided by the EUCS Supplier;
“EUCS Supplier”	a supplier under an agreement between the Authority and a provider of end user computing services under the FITS Programme;
“Event Management System”	an automated system used to track and manage the status of Event Records throughout the Event lifecycle;
“Exception”	a deviation of project tolerances in accordance with PRINCE2 methodology in respect of the Agreement or in the supply of the Hosting Services and/or the FITS Services;
“Exceptional Bonuses”	the exceptional bonuses Bounded Mechanism as further described in paragraph 7.9 of schedule 7.1 (Charging and Invoicing);
“Exclusive Assets”	those Assets which are used exclusively in the provision of the Hosting Services and identified as such in the Register(s) and/or the Asset Register;
“Exit Management”	the obligations and rights of the respective parties pertaining to managing a smooth transition from the provision of the Hosting and/or FITS Services by the Hosting Supplier to the provision of Replacement Services by the Authority or any Replacement

Term	Definition
	Hosting Supplier, all as set out in schedule 8.5 (Exit Management);
“Exit Management Plan”	the Exiting Suppliers’ documentation that sets out the timetable, approach, tasks and responsibilities for achieving an orderly exit and overall management of the service transfer arrangements from an Exiting Supplier to a FITS Supplier;
“Exit Management Services”	any and all of the services to be provided by the Hosting Supplier under schedule 8.5 (Exit Management);
“Exit Manager”	the person appointed by each party pursuant to paragraph 2.5 of schedule 8.5 (Exit Management) for managing the parties’ respective obligations under schedule 8.5 (Exit Management);
“Exit Obligations”	the terms and conditions of exit applicable to the Exiting Suppliers’ or FITS Suppliers’ agreements;
“Exit Plan”	the plan produced and updated by the Hosting Supplier during the Term in accordance with paragraph 4 of schedule 8.5 (Exit Management);
“Exiting Contracts”	the Authority’s agreements, including the 2020 Hosting Agreement;
“Exiting Supplier”	a Supplier with whom the Authority has an Exiting Contract;
“Exiting Supplier ICT Environment”	the ICT Environment used by an Exiting Supplier to provide a service under an Exiting Contract;
“Expert”	the person appointed by the parties in accordance with paragraph 18.2 Part B of schedule 3 of the Master Services Agreement;
“Expert Witness”	a member of a UK Expert Witness register;
“Extended Location”	a location where an End User consumes or accesses the End to End Services and/or FITS Services which is not an Authority Site and shall include but not be limited to End Users’ homes and judges’ lodgings;
“Extension Period”	the Authority’s option to extend the Initial Term by a period of up to twelve (12) months;
“Fast-track Change”	any Contract Change which the parties agree to expedite in accordance with paragraph 7 of schedule 8.2 (Change Control Procedure);
“Final Transition Milestone”	the last Milestone relating to Transition to be delivered by a FITS Supplier;
“Financial Distress Escrow Account”	an escrow account established in accordance with schedule 7.4 (Financial Distress) in the joint names of the Hosting Supplier and the Authority with a bank approved by the Authority;
“Financial Distress Event”	the occurrence of one or more of the events listed in paragraphs 3.1, 4.1 and/or 5.1 of schedule 7.4 (Financial Distress);
“Financial Distress Service Continuity Plan”	the plan to be provided by the Hosting Supplier in accordance with schedule 7.4 (Financial Distress), setting out how the Hosting

Term	Definition
	Supplier (together with the Guarantor and/or Key Sub-contractors, where appropriate) will ensure the continued performance and delivery of the FITS Services/ Hosting Services in accordance with this Agreement in the event that the Hosting Supplier, the Guarantor and/or a Key Sub-contractor suffers a Financial Distress Event or a Sub-contractor Financial Distress Event (as applicable);
“Financial Model”	the Base Case Financial Model or where an Updated Financial Model exists, the most recent Updated Financial Model;
“Financial Transparency”	has the meaning given to it in paragraph 2.4 of schedule 7.1 (Charging and Invoicing);
“First Draft Delivery Date”	the planned date by which the Hosting Supplier shall submit a draft Documentary Deliverable to the Authority;
“FITS Programme”	the Authority's Future IT Sourcing Programme;
“FITS Programme Board”	the board responsible for overseeing the FITS Programme and comprised of key stakeholders from across the Authority, as described in paragraph 10.3.2;
“FITS Programme Plan”	the plan that sets out the dates, sequences and dependencies for the Transition Period as further described in schedule 6.1 (Project Management);
“FITS Project Manager”	the officer of the Authority nominated by the Authority to be the project manager of a Project;
“FITS Services”	all the services to be provided by the FITS Suppliers under the Tower Service Agreements, including the Cross Tower Services as set out and defined in the Master Services Agreement;
“FITS Supplier” or “Supplier”	a supplier (including, except where expressly excluded, a Collaborating Supplier) that has entered into a Tower Service Agreement with the Authority and has entered into an Accession Agreement in the form set out in Schedule 1 (Pro-Forma Accession Agreement) of the Master Services Agreement;
“FITS Supplier ICT Environment”	an ICT Environment used by a FITS Supplier to provide the FITS Services;
“FITS Transition Assurance Function”	the temporary organisation provided by the SIAM Supplier to work on behalf of the Authority throughout the End to End Transition to assure the delivery of all Suppliers' Transition obligations;
“FITS Transition Board”	the board described in Appendix C of schedule 6.1 (Project Management);
“FMO Services”	any services provided by Collaborating Suppliers, Other Authority Providers or FITS Suppliers after the final CPP has been achieved under each Tower Services Agreement and the Future Mode of Operation has been achieved;
“FOIA”	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with

Term	Definition
	any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
“Force Majeure Event”	any cause affecting the performance by a party of its obligations arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Hosting Supplier, the Hosting Supplier Personnel or any other failure in the Hosting Supplier or the Sub-contractor's supply chain;
“Forecast Expenses”	all amounts recognised as costs in accordance with generally accepted accounting principles within the United Kingdom but excluding taxation, funding and similar costs, amounts payable under clause 13 of schedule 7.1 (Charging & Invoicing), capital expenditures and non-cash items (including but not limited to depreciation, amortisation, impairments and movements in provisions) as forecast by the Hosting Supplier in the Financial Model to be incurred over the Term and in respect of the Agreement;
“Forecast Gain”	Forecast Revenue less Forecast Expenses;
“Forecast Gain Margin”	Forecast Gain divided by Forecast Revenue and expressed as a percentage;
“Forecast Profit”	the profit earned or forecast to be earned by the Hosting Supplier calculated in the Financial Model;
“Forecast Revenue”	all Charges forecast to be paid or payable to the Hosting Supplier by the Authority in the Financial Model over the Term and in respect of the Agreement;
“Forensic Readiness Planning Scenarios”	a scenario detailing potential security incidents along with typical diagnostic indicators, typical sources of digital evidence, a typical investigation workflow and desired outcomes;
“Forensic Readiness Plans”	the contingency planning and capability building activities associated with implementation of Forensic Readiness Policy. A Forensic Readiness Plan is a document detailing the outcome of the Forensic Readiness Planning process;
“FTAF”	the SIAM Supplier when supplying FTAF Services;
“Fully Functional”	works or operates in accordance with the manufacturer's specifications and tolerances and/or meets all other agreed Authority specifications and quality criteria;
Functional Unit	a unit within the Authority that is responsible for the delivery of a business function, for example: a single Magistrates Court; a single County Court; Service and Supplier Management within Digital and Technology and a business Programme;

Term	Definition
“Future Mode of Operation” or “FMO”	the mode of operation in respect of the FITS Services, or any component thereof, when the relevant services are being delivered and charged in accordance with the relevant TSA(s), in particular: <ul style="list-style-type: none"> (a) the relevant services are being delivered in accordance with schedule 2.1 (Service Requirements) and schedule 2.2 (Service Performance Management) of the relevant TSA(s); (b) no Exiting Suppliers are employed in the delivery of such relevant services (except where there are legacy activities or licensing agreed with the Authority); and (c) the FITS ICT Environments and the relevant FITS Supplier(s)’s ICT Environment(s) are implemented in accordance with the solution set out in schedule 4.1 (Hosting Supplier Solution) of the relevant TSA(s); and (d) the Service Commencement Date has occurred;
“FMO Processes and Procedures”	the processes and procedures carried out by the FITS Suppliers during FMO;
“FPMF”	means the FITS Programme Management Framework and is the governance applicable to the Transition Period and to the delivery of Future Services;
“Future Services”	the services which are to be provided by the Suppliers as requested by the Authority in accordance with the Change Control Procedure and/or clause 11.8 – 11.11 (inclusive) (Future Services);
“Gain Share Amount”	the amount by which the Earned Gain in each Contract Year exceeds the Threshold Gain Margin;
“Gain Share Calculation”	the calculation of the Gain Share Amount as prepared from time to time in accordance with paragraph 13 of schedule 7.1 (Charging and Invoicing);
“Gate 3 Review”	means Gate 3 Review as described in the FPMF;
“GDPR Claim”	a third party claim or investigation or other enforcement action by any regulator for breach of the Data Protection Legislation;
“General Anti-Abuse Rule”	<ul style="list-style-type: none"> a) the legislation in Part 5 of the Finance Act 2013; and b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;
“General Change in Law”	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Hosting Supplier) or which affects or relates to a Comparable Supply;
“Gold Command”	a facility activated to support the management of critical operational incidents which is usually remote from the site in which the incident is taking place;
“Good Industry Practice”	the exercise of that degree of skill, care, prudence, efficiency,

Term	Definition
	foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;
“Grand Future Mode of Operations” or “Grand FMO”	the date when the final CPP Milestone has been Achieved by all FITS Suppliers, all FITS Services and FITS Suppliers’ solutions are in their Future Mode of Operations, and no Exiting Suppliers are employed or engaged (except where there are legacy activities or licensing agreed with the Authority);
“Group”	one or more End Users grouped in accordance with a set of rules including but not limited to rules relating to their functional role and Business Unit;
“Halifax Abuse Principle”	the principle explained in the CJEU Case C-255/02 Halifax and others;
“Hardware Assets”	those assets which are owned by the Authority which the Authority has allowed the Hosting Supplier to use in connection with the provision or receipt of the Hosting and/or FITS Services in accordance with the provisions of clause 10 (Transfer of Assets and Third Party Agreements) and schedule 6.3 (Asset Transfers);
“Health and Safety Regime”	the Food Safety Act 1990 (and associated regulations), the Health & Safety at Work etc. Act 1974 (and associated regulations), the Fire Precautions Act 1971, the Environmental Protection Act 1998, the Water Industry Act 1991, the Water Resources Act 1991 and any similar or analogous health, safety or environmental legislation in force from time to time;
“His Majesty’s Prison and Probation Service” or “HMPPS”	the executive agency of the Authority whose role is to commission and provide offender services in the community and in custody in England and Wales;
“Hosted Applications”	those Applications that are identified as Applications for which the Authority has designated requiring support;
“Hosting Services”	any and all of the services to be provided by the Hosting Supplier under this Agreement, including those set out or referred to in schedules 2.1 (Service Requirements) and 6.1 (Project Management);
“Hosting Supplier Cause”	any breach by the Hosting Supplier of any of its Responsibilities under the Dependencies Registers (except to the extent that it is the result of any act or omission by the Hosting Supplier to which the Authority has given its prior consent);
“Hosting Supplier Equipment”	the hardware, computer and telecoms devices and equipment supplied by the Hosting Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Hosting and/or FITS Services;
“Hosting Supplier ICT Environment”	the ICT Environment used by the Hosting Supplier to provide the Hosting Services;
“Hosting Supplier Material”	the Hosting Supplier Software together with the Documentation relating to the Hosting Supplier Software;

Term	Definition
“Hosting Supplier Personnel”	all employees, agents, consultants and contractors of the Hosting Supplier and/or of any Sub-contractor;
“Hosting Supplier Representative”	the representative appointed by the Hosting Supplier pursuant to clause 23.1 (Representatives);
“Hosting Supplier Site”	Sites owned, controlled or occupied by the Hosting Supplier which are used for the delivery by the Hosting Supplier or its Sub-contractors for the provision of Hosting Services;
“Hosting Supplier Software”	software which is proprietary to the Hosting Supplier and/or any Affiliate of the Hosting Supplier, including software which is or will be used by the Hosting Supplier for the purposes of providing the Hosting Services and/or FITS Services including the software specified as such in schedule 5.1 (Software);
“Hosting Supplier Solution”	the Hosting Supplier’s solution for the Services attached to this Agreement at schedule 4.1 (Hosting Supplier Solution);
“Hosting Supplier's Background IPRs”	<p>(a) IPRs owned by the Hosting Supplier before the Effective Date, for example those subsisting in the Hosting Supplier's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Hosting Supplier's Know-How or generic business methodologies;</p> <p>(b) IPRs created by the Hosting Supplier independently of this Agreement; and/or</p> <p>(c) IPRs subsisting in any Hosting Supplier Software which is embedded in or which is an integral part of the Specially Written Software together with any IPRs subsisting in any Hosting Supplier Material related to that Hosting Supplier Software,</p> <p>but excluding IPRs owned by the Hosting Supplier subsisting in the Hosting Supplier Software which are not covered under paragraphs (a) to (c) above;</p>
“Hosting Supplier's Change Manager”	the person appointed to that position by the Hosting Supplier from time to time and notified in writing to the Authority or, if no person is notified, the Hosting Supplier’s Representative;
“Hosting Supplier's Confidential Information”	any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of the Hosting Supplier, including IPRs, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as “confidential”) or which ought reasonably to be considered to be confidential, including the Commercially Sensitive Information;
“Hosting Supplier's Group”	the Hosting Supplier, its ultimate holding company and all subsidiaries of its ultimate holding company, the definitions of “holding company” and “subsidiary” being those set out in

Term	Definition
	sections 1159, 1160 and schedule 6 of the Companies Act 2006;
“Hosting Transition Function”	the Hosting Supplier function required to deliver the obligations and requirements set out in schedule 6.1 (Project Management);
“Hosting Transition Period”	means the period of time beginning on the Effective Date and ending on Grand FMO;
“Hosting TF Services”	the services provided by the Hosting Supplier in accordance with requirements set out in schedule 6.1 (Project Management);
“HR Policies”	the Authority's human resources policies as identified in schedule 11 (Referenced Documents);
“ICT Data Model”	the collection of logical “concepts” (things, terms, etc.) and “relationships” between them that describes an ICT domain. The FITS ICT Data Model is a conformed sub-set of a broader Enterprise Architecture meta-model. Generically, it provides a common language for describing the FITS ICT domain and business functions. Specifically, it informs the data standards and data schemas that enable information integration across system boundaries;
“ICT Environment”	an information and communications technology systems environment (consisting of hardware, software and/or telecommunications networks or equipment) which is used by the Authority to receive End to End Services, including Live Environments and Non-Live Environments;
“IDAM Connector”	a component of the IDAM Service that enables the synchronisation of identity attributes between the IDAM Service and other systems;
“IMACD”	shall mean all installations, moves, additions, changes and disposals to the infrastructure and Software under the control of Change Management;
“Impact Level”	has the same meaning as Business Impact Level;
“Incentive Schemes”	the incentive schemes Bounded Mechanism as further described in paragraph 7.8 of schedule 7.1 (Charging and Invoicing);
“Incident”	any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service;
“Incident Resolution”	the action taken to repair the cause(s) of an Incident or to implement a workaround to the satisfaction of the Authority;
“Incident Resolution Priority”	the incident resolution priority categories set out in the SIAM Supplier's Incident Management Policies, Processes and Procedures;
“Incident Resolution Time”	the time taken to achieve Incident Resolution following the occurrence of an Incident;
“Index” or “Indexation”	the adjustment of an amount or sum in accordance with paragraph 2A of schedule 7.1 (Charging and Invoicing);

Term	Definition
“Information”	for the purpose of clause 44, has the meaning given under section 84 of the Freedom of Information Act 2000;
“Information Asset”	any item of information, whether written, printed, spoken, recorded or processed electronically, that has value to the Authority;
“Information Assets Register”	the Authority's register detailing the Authority's information Assets;
“Information Assurance Maturity Model”	the tool used by the Government to assess the effectiveness of the implementation of the Security Policy Framework Mandatory Requirements. Generally, the IAMM process is used to assess the maturity of Information Risk Management across an organisation;
“Information Commissioner Office”	the UK's Information Commissioner's Office;
“Information Management Strategy”	the approach chosen to capture, manage, store, access, use, circulate and delete information;
“Information Security Management”	the process that ensures the confidentiality, integrity, and availability of the Authority's Assets, Information, data and FITS Services. Information Security Management forms part of the Authority's approach to Security Management, which has a wider scope than the FITS Supplier, and includes handling of paper, building access, phone calls, and so forth, for the entire organization;
“Information Security Management System”	has the meaning given to it in schedule 2.5 (Security Requirements);
“Information System”	an Information System (IS) is a coherent set of processing and Information Assets. Typically including the automation of business processes and the creation, reading, updating and deleting of information associated with the processes. An Information System will process inputs (information and business events) produce outputs (information and business events) to and from a variety of agents including users and other systems. It requires Information Technology;
“Information Technology”	a platform for Information Systems of co-ordinated resources to enable and manage inputs, outputs, execution of automated processes and storage and retrieval of information. IT typically includes common capabilities shared between Information Systems including central processing units, memory, devices, operating system and application platform software;
“Infrastructure Directory”	the technical directory used by the ICT Environment for authentication and authorisation;
“Initial Term”	the period from the Effective Date up to and including 18 th May 2024;
“Insolvency Event”	the occurrence of any of the following events (or any event analogous to any of the following in a jurisdiction other than

Term	Definition
	<p>England and Wales) in relation to the relevant entity:</p> <ul style="list-style-type: none"> (a) the entity passing a resolution for its winding up or a court of competent jurisdiction making an order for the entity to be wound up or dissolved or the entity being otherwise dissolved; (b) the appointment of an administrator of or, the making of an administration order in relation to the entity or the appointment of a receiver or administrative receiver of, or an encumbrancer taking possession of or selling, the whole or part of the entity's undertaking, assets, rights or revenue; (c) the entity entering into an arrangement, compromise or composition in satisfaction of its debts with its creditors or any class of them or takes steps to obtain a moratorium or makes an application to a court of competent jurisdiction for protection from its creditors; (d) the entity being unable to pay its debts or being capable of being deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or (e) the entity entering into any arrangement, compromise or composition in satisfaction of its debts with its creditors. <p>However, a resolution by the relevant entity or a court order that such entity be wound up for the purpose of a bona fide reconstruction or amalgamation shall not amount to an Insolvency Event;</p>
“Insurances”	all or any of the insurances required to be maintained by the Hosting Supplier pursuant to this Agreement as set out in schedule 2.6 (Insurance Requirements);
“Intellectual Property Rights” or “IPRs”	<ul style="list-style-type: none"> (a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information; (b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and (c) all other rights having equivalent or similar effect in any country or jurisdiction;
“Inter-Domain Gateway”	an Inter-Domain Gateway is used to demarcate the boundary of two or more ICT Environments that have different risk profiles or Accreditation scopes, and manage Information Assets at different Impact Levels or Protective Marking. An Inter-Domain Gateway

Term	Definition
	is used to implement security controls to protect Information Assets held within and transferred between such ICT 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 Hosting Supplier's ICT Environment to public networks and to those provided by Other FITS Suppliers, Other Authority Providers, Collaborating Suppliers and Exiting Suppliers who may or may not be connected to the PSN;
“Interface”	a boundary across which two independent systems can communicate with each other and share data;
“Interoperability Gateway”	an Interoperability Gateway is used to demarcate the boundary of two or more ICT Environments that have different risk profiles or Accreditation scopes, yet manage Information Assets at the same Impact Level or Protective Marking. An Interoperability Gateway is used to implement security controls to protect Information Assets held within and transferred between such ICT Environments. An Interoperability Gateway may be used to connect the Hosting Supplier's ICT Environment to those provided by Other FITS Suppliers, Other Authority Providers, Collaborating Suppliers and Exiting Suppliers who may or may not be connected to the PSN;
“IPR Claim”	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR used to provide the Hosting Services and/or FITS Services or as otherwise provided by the Hosting Supplier (or to which the Hosting Supplier has provided access) to the Authority in the fulfilment of its obligations;
“IS1&2”	the HMG standard for information risk management;
“IT Health Check”	one or more test sets conducted under the Terms and Conditions of the CESG CHECK Scheme attached as an appendix to schedule 11 (Referenced Documents) designed to expose vulnerabilities in the security of the component or system that could otherwise lead to a breach of confidentiality, integrity or availability of an Information Asset;
“IT Health Check Services”	the services provided by the IT Health Check Supplier(s);
“IT Health Check Supplier(s)”	a supplier(s) under an agreement with the Authority for the provision of accredited penetration testers qualified to assess HMG systems up to and including SECRET classification;
“IT Infrastructure Library Framework”	version 3 of the Information Technology Infrastructure Library, as updated in July 2011, as amended or replaced by another industry standard or framework for IT Service Management from time to time;

Term	Definition
“IT Service Continuity” or “ITSC”	the process of ensuring that the availability of defined and agreed FITS Services will be maintained during abnormal situations;
“ITSC Event”	any Event that affects a FITS Service, that triggers the invocation of one of the planned responses defined in the ITSC plan for that service;
“ITSC Event Report”	a written document following an ITSC Event where an Identified FITS Service required the ITSC Plan to be invoked that describes the conditions of invocation, the details of activities undertaken to maintain availability of the FITS Service, explanation for anything deviation from the ITSC Plan and Lessons Learnt for future invocation of the ITSC Plan;
“ITSC Plan” or “Hosting ITSC Plan”	a plan defining the steps required to recover one or more FITS Services following an ITSC Event. The plan also identifies the triggers for invocation, people to be involved, communications etc. The IT Service continuity plan should address the requirements set out in the Business Continuity Plan;
“ITSC Planning Process”	the process by which the IT Service Continuity plans are established to best respond to the requirements set out in the Business Continuity Strategy;
“ITSCM Awareness and Training Plan”	a list of activities to raise awareness for Authority and Suppliers personnel on Service Continuity and to identify and provide focused training on Service Continuity;
“ITSCM Plan” or “Hosting ITSCM Plan”	the list of activities that will be undertaken following an ITSC Event. The ITSCM Plan defines the personnel and sequenced actions as well as communication mechanisms that would be involved in the management of Service Continuity in case of an ITSC Event;
“ITSCM Strategy”	defines the approach chosen to ensure that the FITS Supplier can always meet the agreed Service Levels by reducing the Risk to FITS Services to an acceptable level and planning for the recovery of FITS Services following an ITSC Event;
“ITSCM Testing Schedule”	a list of activities and their associated timescale for the testing of the ITSC Plans;
“ITSM Operations”	the service categories within the Service Register identified as being Band 7;
“ITSM Toolset”	a set of predefined tools used to support the delivery of the FITS Services as defined by and where appropriate provided by the SIAM Supplier;
“ITSM Toolset Interface Standard”	the description of the mechanisms and rules to interconnect with the central ITSM Toolset;
“Joint Insured”	one of the insured in a type of insurance policy covering more than one insured;
“Joint Transition Management Group”	the group described in Appendix C of schedule 6.1 (Project Management) with the functions set out in paragraph 10.3.4 of

Term	Definition
	schedule 6.1 (Project Management);
“Key Milestone”	an ATP Milestone, a SCD Milestone or a CPP Milestone;
“Key Personnel”	those members of the Hosting Supplier Personnel described in schedule 9.2 (Key Personnel) as such may be modified by agreement by the parties from time to time;
“Key Review”	has the meaning given to it in paragraph 8.3.3(b)(ii) of schedule 6.1 (Project Management);
“Key Sub-contract”	each Sub-contract with a Key Sub-contractor;
“Key Sub-contractor”	<ul style="list-style-type: none"> (a) each of the Key Sub-contractors listed in schedule 4.3 (Notified Sub-contractors); (b) any Sub-contractor that has entered into a Sub-contract to replace any Key Sub-contractor listed in schedule 4.3 (Notified Sub-contractors); (c) any Sub-contractor which in the opinion of the Authority performs a business critical role in the provision of the Hosting and/or FITS Services; and (d) any Sub-contractor with a Sub-contract with a contract value in excess of 10% of the aggregate Charges payable under this Agreement;
“Key Users”	a list of defined End Users that have extended access to ITSM material and systems to perform their role, as well as End Users who have the authority to grant authorisation on other End Users to access the End to End Services;
“Know-How”	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Hosting Services and/or FITS Services but excluding know how already in the Hosting Supplier’s or the Authority’s possession before the Effective Date;
“Knowledge Base”	an information repository for the use of the Suppliers and the Authority in support and delivery of FITS Services;
“Knowledge Management Strategy”	the approach to the gathering, analysing, storing and sharing of knowledge, information, experiences and ideas within an Organisation in order to reduce the need to rediscover knowledge;
“LAN”	the data network carrying all computer, voice, video and other data between all end points at a Site and the agreed hand off point of the WAN Supplier(s) where end points are all devices connected to the LAN including, but not limited to; Client Devices, System Devices and Peripheral Equipment;
“Law”	any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, regulatory policy, binding guidance or industry code, judgment of a relevant court of law, or directives or statute, bye-law, regulation, order, regulatory policy, binding guidance or industry code, rule of Court or directives or

Term	Definition
	requirements of any Regulatory Body, delegated or subordinate legislation, and including retained European Union law;
“Law Enforcement Purposes”	has the meaning set out in the DPA 2018;
“Lead Supplier”	the FITS Supplier nominated by the Authority to be the lead supplier in relation to a Project in accordance with the procedure set out in schedule 6.1 (Project Management);
“Level 1 Credit Rating Threshold”	the level 1 Credit Rating Thresholds as set out in Appendix 2 to schedule 7.4 (Financial Distress);
“Level 2 Credit Rating Threshold”	the level 2 Credit Rating Thresholds as set out in Appendix 2 to schedule 7.4 (Financial Distress);
“Level 3 Credit Rating Threshold”	the level 3 Credit Rating Thresholds as set out in Appendix 2 to schedule 7.4 (Financial Distress);
“Licence to Occupy”	the licence to be granted by the Authority to the Hosting Supplier pursuant to clause 69 (Authority Accommodation);
“Licensed Materials”	the Hosting Supplier Software, Hosting Supplier's Background IPR, Third Party Software, Embedded Third Party IPRs;
“Licensee”	the Authority or a Replacement FITS Supplier as applicable;
“Licensor”	the Hosting Supplier or the owner of the Third Party Software as applicable;
"Licensor's Software"	the Hosting Supplier Software, the Third Party Software and/or the Hosting Supplier's Background IPRs (as applicable);
“Liquid Sub-contractor Market”	that there are sufficient willing parties (being at least two parties, each of whom is capable of being a substitute Key Sub-contractor) in the market of similar contracts for the provision of the services (in each case similar to the existing Key Sub-contract) for a price which is fair value;
“Live Data”	all data that is contained within the Live Environment that it is used to support the activity of the Authority; this may include but not be limited to corporate data, financial data, personal data, configuration data;
“Live Environment”	any ICT Environment used by Suppliers, Exiting Suppliers or Other Authority Providers to provide End To End Services or Hosting Services to Users;
“Live Proving Environments”	has the meaning given to it in the Authority Test Strategy;
“Live Proving”	has the meaning given to it in the Authority Test Strategy;
“Local Hosting”	the service categories within the Service Register identified as being Band 2;
“Local Server Room”	a room at an Authority Site that houses System Devices and equipment necessary to deliver End To End Services to End Users at the Authority Sites;
“Lodge Card”	has the meaning given to it in paragraph 8.2 of schedule 7.5 (Financial Model);

Term	Definition
“Loss”	losses, claims, fines, damages, liabilities, costs, charges, expenses, demands, legal and other professional costs;
“Maintenance & Support Environments”	has the meaning given to it in the Authority Test Strategy;
“Malicious Software”	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
“Management Information”	the management information specified in schedule 7.1 (Charging and Invoicing) and schedule 8.1 (Governance) to be provided by the Hosting Supplier to the Authority;
“Manual Accounting Processes”	processes associated with the manual generation of Accounting Items or the manual exporting of Accounting Items or Accounting Logs and the associated analysis;
“Master Application List”	the list of all Business Applications that contains for each one their principal function, business ownership, key stakeholders, and criticality, as included as a Referenced Document;
“Master Directory”	the directory which is the reference database for identities within the Authority providing a common capability for the maintenance and synchronisation of information relating to all identities, roles and access rights. It enables identity data to be sourced from other system directories and databases (including but not limited to human resource and corporate finance); merged into a master set; maintained; and provided to sub-ordinate directory systems including Infrastructure Directories;
“Master Services Agreement”	has the meaning given in paragraph d of the Introduction to this Agreement;
“Master Site List”	the list of Sites and Extended Locations to which FITS Services are delivered including, but not limited to, summary information about Devices, Software, other equipment and services provided to those Sites and Extended Locations;
“Master Time Reference”	a common clock source reference, for example a Stratum 0 device, that allows infrastructure to synchronize its timing such as a Global Positioning System (GPS). The timing is disseminated to the infrastructure using industry standard methods such as Network Time Protocol (NTP);
“Maturity Assessment Approach”	the structured method to measure operational capability in specific disciplines against a defined evaluation criterion. To be used and applied in the delivery of FITS Services and focussed on the optimisation of behaviours, working practices, policies and processes and including a measured maturity continuum to support effective management of improvement across the FITS Services enabling capabilities to be benchmarked and improvement opportunities to be identified;

Term	Definition
“Maximum Service Credit Points to Reach Cap”	the value identified in paragraph 9.2 of Schedule 7.1 (Charging and Invoicing);
“Maximum Delay Payment Period”	where used, the maximum period of time for which Delay Payments will be applied for each Milestone as set out in Table 1, paragraph 4.2 of schedule 7.1 (Charging and Invoicing);
“Mediator”	the independent third party appointed in accordance with paragraph 6.3 Part B of schedule 3 of the Master Services Agreement;
“Metered Service”	a service that is used and subsequently paid for based upon the measured usage; and means the same as the NIST definition of Measured Service (NIST publication SP800-145 published September 2011);
“Middleware”	a set of System Software that facilitates the exchange of data between ICT Environments;
“Milestone”	has the same meaning as “Project Milestone”;
“Milestone Achievement Certificate”	a certificate granted by the Authority when a FITS Supplier has Achieved a Milestone;
“Milestone Date”	the date set against the relevant Milestone set out in the Transition Table;
“Milestone Payment”	a payment identified in schedule 7.1 (Charging and Invoicing) made following the issue of a Milestone Achievement Certificate;
“Mobile Client Device”	the portable hardware utilised by an End User to receive their IT services, including, but not limited to laptops and tablets;
“Mobile Telephony Device”	any Telephony Device capable of delivery of Telephony Services wirelessly;
“Modern Slavery Assessment Tool”	means the modern slavery risk identification and management tool which can be found online at: https://supplierregistration.cabinetoffice.gov.uk/msat
“MoJ Security Policies”	the Authority’s security policies as provided or otherwise made available to the Hosting Supplier from time to time;
“Month” or “month”	a calendar month and “monthly” shall be interpreted accordingly;
“Monthly Risk Review Board”	means the board more particularly described in paragraph 2.10 of schedule 8.1 (Governance);
“MSA Contract Year”	the period of twelve (12) months (or shorter period in the period immediately prior to the end of the MSA contract term) commencing on the effective date of the MSA or on an anniversary of the effective date of the MSA;
“Multi-Tenant (Multi-Tenanted)”	an ICT resource sub-divided into separate allocated portions each occupied by its "tenant" consumer of the resource;
“National Security Vetting”	a requirement set by the Cabinet Office to protect against threats from hostile intelligence services, terrorist groups, organised criminals, and other pressure groups. NSV is used to decide whether an individual can be trusted with sensitive government

Term	Definition
	information or property;
“NCC Escrow International”	NCC Group Escrow Limited, a company registered in England and Wales whose registered office is at Manchester Technology Centre, Oxford Road, Manchester M1 7EF, England (registered number: 3081952);
“Network Device”	any Device used in the provision of WAN or LAN services
“Network Impact Analysis”	network monitoring, analysis of the impact of possible network threats and vulnerabilities;
“Network Services”	the services provided by the Network Supplier;
“Network Supplier”	a supplier under an agreement between the Authority and a provider of network services under the FITS Programme;
“Non-conformance Report”	a report issued by the Authority pursuant to clause 7.1 (Delays due to Hosting Supplier default) which sets out the reasons why any Test has failed or of any non-conformities in respect of any Milestone, Deliverable Documentary Deliverable or other aspect of the FITS Service;
“Non-Documentary Deliverables”	any Deliverables excluding Documentary Deliverables;
“Non-Exclusive Assets”	those Assets which are not used exclusively in the provision of the Hosting Services and identified as such in the Register(s) and/or the Asset Register;
“Non-Live Environment”	any ICT Environment used by Suppliers, Exiting Suppliers or Other Authority Providers for the development and testing of the End to End Services or Hosting Services, Configuration Items, Releases and Processes, including any testing carried out in accordance with the Supplier Test Policy and Authority Test Strategy as well as training in the use of the End to End Services or Hosting Services;
“Notice of Dispute”	a written notice served by one party on the other stating that the party serving the notice believes that there is a Dispute;
“Occasion of Tax Non-Compliance”	<p>a. any tax return of the Hosting Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found to be incorrect as a result of:</p> <ul style="list-style-type: none"> i. a Relevant Tax Authority successfully challenging the Hosting Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; or ii. the failure of an avoidance scheme which the Hosting Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or <p>b. the Hosting Supplier’s tax affairs give rise on or after 1 April</p>

Term	Definition
	2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a penalty for civil fraud or evasion;
“Offender”	a person convicted of a criminal offence and being managed within the Criminal Justice System;
“Offshore Proposal”	the detailed proposal of the provision of FITS Services from a location outside the United Kingdom;
“Open Source Software”	software provided under an open-source licence and used in the provision of the FITS Services;
“Operating Environment”	the Authority System and the Sites;
“Operating Standards”	has the meaning given to it in paragraph 3.2.1 of schedule 2.3 (Standards);
“Operating Systems”	Software that communicates with the Device, directing, controlling and scheduling the use of Device resources by other Software and Users;
“Operational Acceptance Test / Testing”	has the meaning given to it in the Authority Test Strategy;
“Operational Change”	a Change to any FITS Service into the Authority’s ICT Environment that follows the Request for Change process as set out in paragraph 13.3 of schedule 2.1 (Service Requirements) including but not limited to Requests for Change (RFC) including standard, normal and emergency;
“Operational Phase”	the phase in which the Hosting Supplier will deliver FMO Services, identified as such in the Transition Plans and commencing from the CPP Milestone Date for any FMO Service;
“Operator Services”	the provision of services to receive telephone calls to a central number and thereafter to route them to the appropriate Authority telephone extension;
“Ordinary Exit”	any termination of this Agreement which occurs: (i) pursuant to clause 57 (Termination Rights) where the period of notice given by the party serving notice to terminate pursuant to such clause is greater than or equal to six months; or (ii) as a result of the expiry of the Term;
“Organisational Change Plan”	the plan made in relation to staffing requirements as more clearly set out in paragraphs 2.4.48 of schedule 6.1 (Project Management);
“Other Authority Provider”	any other third party which supplies services to the Authority, excluding the Suppliers and the Exiting Suppliers;
“Other Authority Provider ICT Environment”	an ICT Environment used by an Other Authority Provider to provide an End To End Service;
“Other FITS Services”	all FITS Services, excluding the Hosting Services;
“Other FITS Supplier”	FITS Supplier(s), excluding the Hosting Supplier;

Term	Definition
“Other Suppliers”	Suppliers excluding the Hosting Supplier;
“Other Tower Bidders”	a bidder who has been invited to negotiate or tender for a Tower Service Agreement by the Authority, but excluding the Hosting Supplier;
“Other Tower Service Agreement”	a Tower Service Agreement between the Authority and an Other FITS Supplier, excluding this Agreement;
“Overhead”	those costs which are intended to recover a proportion of the Hosting Supplier's indirect corporate costs, which shall not include any Base Costs or Capital Costs or any cost separately included in the Base Cost or Capital Cost;
“Partial Termination”	the partial termination of this Agreement to the extent that it relates to the provision of any part of the Hosting Services and/or Cross Tower Services;
“Passive Network Taps”	a hardware device which provides a mechanism to access data flowing across a computer network whilst functioning as a one way data diode;
“Payment Schedule”	the schedule detailing all anticipated Charges to be provided by the Hosting Supplier in accordance with paragraph 7 of schedule 7.5 (Financial Model);
“Penetration Test Process”	ethical Hacking test, a method of evaluating the security of a computer system or network by simulating a malicious attack;
“Peripheral Equipment”	the hardware, other than Client Devices, directly utilised by an End User in order to receive the End to End Services;
“Person Day”	7.5 Person Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
“Person Hours”	the hours spent by the Hosting Supplier Personnel properly working on the Hosting and/or FITS Services including time spent travelling (other than to and from the Hosting Supplier's offices, or to and from the premises at which the services are to be principally performed) but excluding lunch breaks;
“Personal Data”	shall have the same meaning as set out in the Data Protection Legislation;
“Personal Data Breach”	has the meaning set out in Article 4 of the UK GDPR;
“Pilot Test / Testing”	has the meaning given to it in the Authority Test Strategy;
“Planned Approval Date”	the planned date by which a Documentary Deliverable should achieve Approval, as set out in the Document Review Plan;
“Planned Business Change”	the known, agreed and anticipated modifications of business activities;
“Planned Outages”	any time within the service hours when the applicable FITS Service will not be available for use and which has been agreed in advance by the Authority;

Term	Definition
“Planned Unavailability”	the unavailability of infrastructure or Hosting Services that has been agreed in advance by the Authority;
“Platform”	the combination of a System Device and its associated Software; together providing an environment in which Software can be executed;
“PMC Config”	details which recordable events for each PMC are to be recorded, which are to be reported on and which are to be alerted on for every monitored device/log source;
“Post Transition Contract Compliance Rectification Plan”	the plan for the rectification of all identified areas of non-compliance with contracted service delivery that is to be implemented by the Hosting Supplier pursuant to schedule 6.1 (Project Management);
“Power over Ethernet (PoE)”	the IEEE standard for powering network devices via Ethernet cable as defined by the standard IEEE 802.3af or successor standards;
“Power Usage Effectiveness” (PUE / DCiE)	Power Usage Effectiveness (PUE) and its reciprocal Data Centre infrastructure Efficiency (DCiE) are widely accepted benchmarking standards proposed by the Green Grid to help IT Professionals determine how energy efficient data centres are, and to monitor the impact of their efficiency efforts;
“Previous Contractor”	a contractor supplying services to the Authority before the Effective Date that are the same as or substantially similar to the Hosting Services (or any part of the Hosting Services) and shall include any subcontractor of such contractor (or any sub-contractor of any such sub-contractor);
“Primary Service Commencement”	the Service Commencement Date for the first FITS Service to be cut over by a FITS Supplier;
“PRINCE 2”	the Projects in Controlled Environments project management method used as a standard across the UK Government;
“Print Services”	the services provided by the Print Supplier;
“Print Supplier”	a supplier under an agreement with the Authority for print services under the FITS Programme;
“Priority 1 Incident”	an Incident which involves a complete or partial loss of service or functionality affecting multiple End Users and/or unavailability of one or more Business Applications, at one or more locations, resulting in a critical business impact that prevents a Functional Unit from working;
“Priority 2 Incident”	an Incident that involves a complete or partial loss of service or functionality affecting multiple End Users and/or complete or partial unavailability of one or more Business Applications, at one or more locations, and results in an important business impact that allows a Functional Unit to do some work but not to complete that work;

Term	Definition
“Priority 3 Incident”	an Incident that involves a complete or partial loss of service or functionality affecting multiple End Users and/or complete or partial unavailability of one or more Business Applications, at one or more locations, where a workaround is not available, resulting in a non-critical business impact on a Functional Unit in that the service or functionality is used by the Functional Unit but is not required for the Functional Unit to complete its function;
“Priority 4 Incident”	an Incident that impacts directly upon a single End User, where an immediate workaround is not available, and there is a non-critical business impact;
“Priority Levels”	a category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken;
“PRISM”	Post Release Implementation Support and Maintenance. A period, post implementation, of continued support in Live Environment from a FITS Supplier or Other Authority Provider;
“Problem Management System”	an automated system used to track and manage the status of Problem Records;
“Product Description”	<p>(a) a document describing a project Deliverable in the form set out in Annex A of schedule 8.7 (Document Approval Process) or in respect of the Transition Documentary Deliverables, the form set out in Appendix B of schedule 6.1 (Project Management) and according to content specified by the Authority; or</p> <p>(b) a description of a product's purpose, composition, derivation and quality criteria, produced at planning time, once the need for the product is identified, in a form and according to content specified by the Authority;</p>
“Programme Test Strategy”	has the meaning given to it in the Authority Test Strategy;
“Project”	means a temporary organisation with people and other assets, that is required to achieve an objective or other outcome;
“Project Authority Notice to Proceed Date”	the date from which the Authority has confirmed that the relevant parties can commence a Project in accordance with schedule 6.1 (Project Management);
“Project Authority to Proceed”	a notice issued by the Authority pursuant to paragraph 1.11.2.1 of Part 2 of schedule 6.1 (Project Management);
“Project Impact Statement”	a statement from the Hosting Supplier and all other relevant FITS Suppliers (as applicable) setting out the impact (if any) on their cost models, Charges, resources, Transition Table of schedule 6.1 (Project Management) and Table 1 (Delay Payments for Milestones) of schedule 7.1 (Charging and Invoicing) in relation to the Transition Documentary Deliverables for a Project in accordance with the procedure set out in schedule 6.1 (Project Management);

Term	Definition
“Project Initiation Document”	a document in a form and according to content specified by the Authority that sets out scoping information relating to a project, including any Acceptance Criteria relating to a project;
“Project Milestone” or “Milestone”	an event or task described in the Transition Portfolio Plan, in a Transition Plan or in a Project Plan as a “Milestone” which, if applicable, must be completed by the relevant Milestone Date, including milestones in respect of any ATP, SCD and CPP;
“Project Notification”	the notification provided by the Authority on initiation of a Project, and including the information set out in paragraph 1.9.2 of schedule 6.1 (Project Management);
“Project Plan”	a statement of how and when a Project's objectives are to be achieved, by showing the major products, Milestones, activities, Deliverables and resources required on the Project;
“Project Specific IPRs”	<p>(a) IPRs in items created by the Hosting Supplier (or by a third party on behalf of the Hosting Supplier) specifically for the purposes of this Agreement and updates and amendments of these items; and/or</p> <p>(b) IPRs arising as a result of the performance of the Hosting Supplier's obligations under this Agreement;</p> <p>but which shall not include the Hosting Supplier's Background IPRs or the Specially Written Software;</p>
“Project Suite”	in respect of any Project, the Project Suite is the Transition Documentary Deliverables and the Project Notification;
“Project Test Plan”	has the meaning given to it in the Authority Test Strategy;
“Project Test Strategy”	the test strategy for a Project as described in schedule 6.1 (Project Management);
"Proposal Document"	a response to a Request for Service made in accordance with the Change Management procedure set out in the SIAM Supplier's Change and Evaluation Management Policies, Processes and Procedures;
“Protective Marking”	<p>a marking scheme to identify the sensitivity of information for an Information Asset; in Government ICT the protective markings are:</p> <p>(a) OFFICIAL;</p> <p>(b) SECRET; and</p> <p>(c) TOP SECRET;</p>
“Protective Measures”	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measures adopted;

Term	Definition
“Protective Monitoring Policy”	a document which describes the principles and high level requirements relating to the delivery of Protective Monitoring Services;
“Protective Monitoring Resolution Plan”	a detailed proposal which describes the activities and resources needed and timescales to mitigate the findings listed in the Digital Forensics Report;
“Protective Monitoring Service”	the services provided by the Protective Monitoring Supplier;
“Protective Monitoring Supplier”	a supplier under an agreement between the Authority and a provider of protective monitoring services under the FITS Programme;
“Protectively Marked Assets”	Information Assets that bear a marking or classification to denote its sensitivity or value to the Authority and the handling requirements in accordance with the Security Policy Framework and/or the Authority's information handling guidance;
“Protectively Monitored Device”	a Device which is monitored by the Protective Monitoring Supplier;
“Protectively Monitored Software”	Software which is monitored by the Protective Monitoring Supplier;
“PSN Security Officer”	the individual responsible for ensuring that the Authority maintains PSN compliance for a set of environments or services, and identifies, manages, escalates and resolves any potential or actual security-related risks or issues that may affect PSN compliance status, as outlined in the PSN Protective Monitoring & Security Incident Management Strategy Public Sector Network Programme Version 1.3;
“Public Key Infrastructure”	a set of policies, processes and procedures, Software and Devices used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates, in accordance with the HMG IA Standard No. 4 Management of Cryptographic Systems;
“Quality Assurance”	the Process responsible for ensuring that a FITS Service and its associated Processes are continuing to deliver their intended value;
“Quality Assurance Review”	an inspection of the Hosting Supplier implementation of the Hosting Services to ensure the adherence to the contractual standards;
“Quality Criteria”	the criteria for Approval by the Authority of a Documentary Deliverable, including any criteria set out in the Product Description for that Documentary Deliverable. In respect of Transition Documentary Deliverables, the Quality Criteria are also set out in Appendix B to schedule 6.1 (Project Management);
“Quality Manager”	the Hosting Supplier’s representative responsible for ensure that the Hosting Supplier adheres to the Quality Plan;

Term	Definition
“Quality of Service”	the ability to prioritise selected network traffic or data flows including but not limited to Business Application data, Messaging data, Telephony Services, Video Conferencing Services;
“Quality Plans”	the Hosting Supplier's plan that reflects the quality management systems as further described in clause 15 (Quality Monitoring);
“Quarter”	the first three months and each subsequent three months until the end of the Agreement;
“Quarterly Business Forecast”	a snapshot of the demand pipeline representing a forecast for demand for services by the Authority. This is produced at regular intervals by the Authority to describe future developments and changes the Authority is planning to undertake;
“Quarterly Capacity Plan”	a list of activities with associated timescales that will be conducted to manage the resources required to deliver FITS Services. The Quality Capacity Plan will be produced every quarter and will contain scenarios for different predictions of business demand, and costed options to meet the agreed Service Level Targets;
“Quarterly Scan Report”	a light touch IT Health Check to be performed quarterly;
“Rating Agencies”	the rating agencies listed in Appendix 1 to schedule 7.4 (Financial Distress);
“Reasonable Recommendation”	a reasonable recommendation notified in writing to the Authority by the Hosting Supplier who shall be acting in good faith and in accordance with Good Industry Practice, to modify the systems and services provided by the Hosting Supplier, for the purpose of managing a genuine and legitimate data security or Data Loss Event risk, which is proportionate to the course of action being recommended;
“Receiving Party”	the party which receives a proposed Contract Change;
“Reconciliation”	a reconciliation of Earned Expenses and Earned Revenue, against the Forecast Expenses and Forecast Revenue set out in the Updated Financial Model compiled from time to time (and in any event upon termination or expiry of this Agreement) in accordance with paragraph 5 of schedule 7.5 (Financial Model);
“Recovery Plan”	the Hosting Supplier’s plan for the remediation of any Service Failure and/or Service Level Failure in accordance with clause 12 (Service Levels);
“Referenced Document(s)”	the documents listed in schedule 11 (Referenced Documents);
“Registers”	has the meaning given to it in paragraph 2.1 of schedule 8.5 (Exit Management);
“Regulatory Bodies”	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Agreement or any other affairs of the Authority and “Regulatory

Term	Definition
	Body ” shall be construed accordingly;
“Release and Deployment Management Strategy”	the approach for planning, scheduling and controlling the build, test and deployment of releases, and for delivering new functionality required by the Authority while protecting the integrity of existing FITS Services;
“Release Event”	events which will trigger the release of the Deposited Software to a duly authorised officer of the Authority;
“Release Plan”	has the meaning given to it in paragraph 5.11.8 of schedule 6.1 (Project Management);
“Release Test Plan”	has the meaning given to it in the Authority Test Strategy;
“Relevant Conviction”	a Conviction that is relevant to the nature of the Hosting and/or FITS Services to be provided including but not limited to those involving dishonesty, violence, sexual offences;
“Relevant Tax Authority”	HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the Hosting Supplier is established;
“Remedial Plan”	the plan referred to in clause 58 (Remedial Plan Process) to correct a material Default;
“Remedial Plan Process”	the process set out in clause 58 (Remedial Plan Process);
“Remote and Mobile Access”	the ability to gain connection to the Authority’s ICT Environments from any site or remote location;
“Removable Media”	hardware and / or material that is capable of providing data permanence, but which can be detached from fixed Service Assets and carried away from the user workplace;
“Repair”	has the meaning given to it in the Authority Test Strategy;
“Replacement FITS Supplier”	any supplier who provides services which are the same as or similar to the Hosting Services following the expiry or termination (in whole or in part) of this Agreement;
“Replacement Hosting Services”	any services which are substantially similar to any of the FITS Services and which the Authority receives in substitution for any of the Hosting Services following the expiry or termination or Partial Termination of this Agreement, whether those services are provided by the Authority internally and/or by any third party;
“Replacement Hosting Supplier”	any third party service provider of Replacement Hosting Services appointed by the Authority from time to time;
“Reporting Period”	a Month;
“Representatives”	either or both of the Authority Representative and the Hosting Supplier Representative;
“Request for Information”	a request for information or an apparent request under the FOIA or the Environmental Information Regulations;
“Request for Service”	a request made by the Authority to commission services which may include additions to the Service Catalogue or require a

Term	Definition
	Change via the Change Control Procedure;
“Request Fulfilment”	the service categories within the Service Register identified as being Band 7;
“Requesting Party”	the party which requests a Contract Change;
“Required Action”	has the meaning given in clause 62.7.1 (Step-In Rights);
“Requirements Document”	a description of the Authority’s requirements for a Project as described in part 2 of schedule 6.1 (Project Management);
“Resolution Plan”	a plan of actions agreed with the Authority to investigate, diagnose, resolve, and prevent future occurrences of an actual or potential breach of security discovered during a security audit, or a failure to comply with Connection Criteria;
“Resolver Group”	a group of appropriately qualified specialists from Suppliers that are nominated in accordance with Good Industry Practice to perform the resolution of Incidents;
“Revised Milestone Date”	any revised date which is set for the Achievement of a Milestone;
“Risk Analysis”	the process of defining and analysing the risk to FITS Service to the Authority, identifying threats to those FITS Service, and evaluating how vulnerable each FITS Service is to those threats;
“Risk History”	the complete catalogue of the R&I Log;
“Risk Management and Accreditation Documentation Set”	the documentation, often a portfolio, which specifies the risk management measures, accreditation policy, and status of an ICT system;
“Risk Management Document”	a document containing all the information about a risk, from the point of first identification, all the way through its life, providing the complete and current information about the risk, including probability and impact estimates or measures, possible mitigation or other risk response, decisions taken (including by whom and with what reasoning), ownership, and actions to monitor status and to communicate information about the risk;
“Risk Register”	a summary and index of all the risk documents that apply to a given system;
“Rough Order of Magnitude”	a rough estimate of time, cost and effort that would be required to fulfil and in support of a request for a Proposal Document;
“Round Robin Database”	a data store which uses a circular buffer and typically reduces the resolution of historical data to allow for new data to be added without increasing the size of the database;
“SCD Milestones”	a Milestone which identifies the Service Commencement Date, as set out in the Transition Table;
“Secure Remote Access”	the connectivity for Client Devices to access End to End Services via public telephony (including but not limited to PSTN, ADSL, and 3G/4G), Internet, and wireless networks;
“Security Accreditation”	a formal document to be completed in order to engage the services

Term	Definition
Engagement Template	of the Accreditor;
“Security Breach”	a Security Incident in which an Information Asset's confidentiality, integrity or availability are compromised;
“Security Content Automation Protocol” (SCAP)	a method using a suite of selected open standards that enumerate software flaws, security related configuration issues, and product names to enable automated vulnerability management, measurement, and policy compliance evaluation;
“Security Event”	an event requiring escalation to the security team;
“Security Incident”	the act of breaching an explicit or implied security policy;
“Security Incident Database”	a complete database of security incidents;
“Security Incident Resolution Plan”	a plan of actions agreed with the Authority to investigate, diagnose, resolve, and prevent future occurrences of a Security Incident;
“Security Investigation”	activities that aim to discover the underlying cause of a Security Incident escalated to the Security Team. Each Security Investigation has its own Terms of Reference (TOR);
“Security Management Plan”	the Hosting Supplier's security plan prepared pursuant to paragraph 5 of schedule 2.5 (Security Management Plan) and referenced in Appendix 1 of schedule 2.5 (Security Management Plan);
“Security Policy Framework”	the Cabinet Office Security Policy Framework;
“Security Risk”	a risk arising from the threat or compromise to an information asset's confidentiality, integrity or availability;
“Security Services”	the services provided by the Security Supplier(s);
“Security Supplier(s)”	a supplier under an agreement between the Authority and a provider of information security services under the FITS Programme;
“Security Team”	the Authority Personnel responsible for handling Security Incidents;
“Self Service Portal”	a system providing access to a selection of FITS Services for users to consume without interaction with Service Desk personnel;
“Service”	a FITS Service, Cross Tower Service or Transition Service as applicable;
“Service Acceptance Test”	has the meaning given to it in the Authority Test Strategy;
“Service Asset”	any resource or capability that contributes to the delivery of a FITS Service;
“Service Catalogue”	the service catalogue developed, maintained and implemented by the SIAM Supplier as described in schedule 2.1 (Service Requirements) and paragraph 5.14 of schedule 6.1 (Project Management);
“Service Charges”	period payments made in accordance with schedule 7.1 (Charging

Term	Definition
	and Invoicing) in respect of the supply of the Hosting Services;
“Service Commencement Date”	the date on which the Authority has agreed that a FITS Supplier or FITS Suppliers may commence the delivery of a FITS Service or Cross Tower Service. This date shall be linked to the Project Milestone and which is defined as an "SCD Milestone" in the Transition Table;
“Service Credit Regime”	the Authority's regime for Service Credits set out in schedule 2.2 (Service Performance Management);
“Service Credits”	the sums payable in respect of the failure by the Hosting Supplier to meet one or more Service Levels as specified in schedule 7.1 (Charging and Invoicing);
“Service Delivery Lifecycle”	the management of the various stages in the life of a FITS Service or End to End Service. The SDLC involves a number of management practices to ensure that FITS Services are provided as agreed between the FITS Supplier and the Authority;
“Service Desk”	the single point of contact between the FITS Supplier and the users;
“Service Failure”	any Default in the provision of a FITS Service;
“Service Handover Pack”	a set of all information, documentation and products detailing the responsibilities for operating a FITS Service in the Authority's ICT Environment;
“Service Hours”	the standard service hours, which are 0700-1830 on Monday to Friday and 0700-1400 on Saturdays and public holidays (excluding Good Friday and Christmas Day);
“Service Knowledge Library”	the Authority's collection of artefacts that describe different aspects of and abstractions of the current Authority's ICT Environment. The SKL will become subsumed into the SKMS after Effective Date;
“Service Level”	the the applicable levels of service required to be provided, as set out in schedule 2.2 (Service Performance Management);
“Service Level Agreement Monitoring View”	a service level agreement monitoring display used to help monitor and report achievements against Service Levels;
“Service Level Failure”	a failure to deliver any part of the Hosting Services in accordance with the applicable Service Levels;
“Service Level Framework”	the framework referred to and encapsulated within schedule 2.2 (Service Performance Management);
“Service Level Target(s)”	the targets described in schedule 2.2 (Service Performance Management);
“Service Level Threshold”	the applicable level below which the quality of any Hosting Services becomes unacceptable to the Authority as set out in schedule 2.2 (Service Performance Management);
“Service Management Framework”	the way in which the full scope of service integration and service management accountabilities, responsibilities and supporting

Term	Definition
	processes are deployed, managed and controlled in a multi-supplier structure across all suppliers and the Authority;
“Service Performance Management”	the services to be provided by the FITS Suppliers to manage the performance of the FITS Services, as prescribed by schedule 2.2 (Service Performance Management);
“Service Readiness Criteria”	the criteria against which a FITS Supplier is assessed prior to being granted ATP and assuming responsibility for the delivery of a service, or component thereof;
“Service Readiness Review”	shall mean the process for <ul style="list-style-type: none"> (a) assessing the FITS Suppliers’ progress in delivering their obligations; (b) assessing the extent of the FITS Suppliers’ outstanding activities to be completed to achieve completion of Service Transition by the relevant Service Commencement Date; (c) identification of any business or End to End Service continuity risks and issues; (d) confirming the Service Commencement Date; and (e) provide recommendation to the Authority for the issue of an ATP;
“Service Register”	is the service register set out in the Dependencies Register;
“Service Request”	a request for information or advice or access or consumption of a FITS Service from the FITS Service Catalogue;
“Service Requirements”	the Authority's requirements as set out in schedule 2.1 (Service Requirements);
“Service Transfer Test Incident Log”	a Test Incident Log established and maintained for the transfer of a FITS Service;
“Service Transfer Test Strategy”	a test strategy setting out the approach to testing for the transfer of a Service from one supplier to another, to be produced, managed and maintained by the Hosting Supplier in accordance with the Authority Test Strategy;
“Service Unavailability”	any period of time during which there is no Service Availability for any End to End Service, FITS Service or Business Application;
“Service Validation and Testing Policies and Procedures”	has the meaning set out in schedule 2.1 (Services Requirements);
“Services Employees”	those employees of the Hosting Supplier who shall from time to time be engaged in the performance of the Services in the relevant part of the undertaking within the Hosting Supplier and who may be transferred on the expiry or termination of this Agreement under the Employment Regulations to the Authority or a Replacement FITS Supplier;

Term	Definition
“Share”	has the meaning given to it in schedule 8 (Definitions) of the Master Services Agreement;
“Shared Hosting Environment”	a subset of Shared Platform within the context of Hosting Services;
“Shared Incentive Fund”	has the meaning given in paragraph 7.8.1 of schedule 7.1 (Charging and Invoicing);
“Shared Platform”	a Platform, where two or more consumers of the Platform resources share the same resources;
“Shared Risk Pots”	the shared risk pots Bounded Mechanism as further described in paragraph 7.7 of schedule 7.1 (Charging and Invoicing);
“SIAM Services”	the services provided by the SIAM Supplier;
“SIAM Supplier”	a supplier under an agreement between the Authority and a provider of SIAM services under the FITS Programme;
“SIAM Transition Function”	the delivery by the SIAM Supplier of the Transition Plans, Transition Solutions and the Deliverables as obligated in the SIAM Tower Services Agreement, but not including the FITS Transition Assurance Function;
“Silver Command”	a secondary control room in an Authority Site which can serve as a back- up to the control room, or be used to support the remote management of incidents within that site;
“Sites”	any location used for the consumption of the FITS Services by an End User;
“SLA Framework”	a structure to serve as support for the definition of Service Levels Targets and the creation of their associated SLA;
“Smartphone”	any Mobile Telephony Device capable of providing Application functionality;
“SME”	an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
“Software”	the Specially Written Software, Hosting Supplier Software, Third Party Software, Open Source Software or Commercial Off The Shelf Software, used in the provision of FITS Services;
“Solution Architecture”	data documents and models defining, describing, modelling, mapping and communicating the as-is and to-be business requirements, business functions, IS/IT systems and service related to the implementation of specific and discrete real-world solutions and change projects;
“Source Code”	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all technical information and documentation necessary for the use, reproduction, modification and enhancement of such software;

Term	Definition
“Specialist Security Services”	the services provided by the Protective Monitoring Supplier, the Digital Forensics Supplier(s), and the IT Health CHECK Supplier(s);
“Specially Written Software”	any programs, codes and software created by the Hosting Supplier (or by a third party on behalf of the Hosting Supplier) specifically for the purposes of this Agreement and/or for use by the Hosting Supplier specifically in the provision of the Hosting Services or the FITS Services (including any modifications or enhancements made to such Software during the Term), including (but not limited to) the items detailed in paragraph 2 of schedule 5.1 (Software);
“Specific Change in Law”	a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
“Staff Transfer”	the transfer of staff under this Agreement pursuant to the Employment Regulations;
“Staff Vetting Procedures”	the Authority's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, as set out in the SKL and including but not limited to, the provisions of the Official Secrets Act 1911 to 1989;
“Stage Payment”	any payment made in respect of a Milestone or on any other date in either case as identified in schedule 7.1 (Charging and Invoicing);
“Standard Application”	a Business Application denoted as such within the Master Application List, but typically with the following characteristics: a Business Application for which a degradation or loss of the service would impact on the productivity of a Business Unit or group of End Users;
“Standard Change”	a pre-approved change item which has a known cost, known procedure for delivery and is contained within the FITS Service Catalogue;
“Standard Licence Terms”	the licence terms set out in Part A (Standard Licence Terms) of schedule 5.2 (Licence Terms);
“Standard Testing Toolset”	the standard testing toolset comprises an integrated set of mandatory and optional tools for the planning, design, execution, reporting and control & monitoring of tests. It includes tools for test management, automation, performance/load testing and defect management;
“Standards”	the British or international standards, Authority's internal policies and procedures, Government codes of practice and guidance referred to in schedule 2.3 (Standards) together with any other specified policies, guidance or procedures identified in schedule 2.3 (Standards) or schedule 2.5 (Security Management Plan);

Term	Definition
“Statement Of Applicability”	a Statement of Applicability under ISO27001/2;
“Step-In Notice”	has the meaning in clause 62.6;
“Step-Out Date”	has the meaning in clause 62.10.2;
“Step-Out Notice”	has the meaning in clause 62.10;
“Step-Out Plan”	has the meaning in clause 62.11;
“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Sub-contract”	any contract or agreement or proposed contract or agreement between the Hosting Supplier and any third party whereby that third party agrees to provide to the Hosting Supplier the Hosting and/or FITS Services or any part thereof or facilities or services necessary for the provision of the Hosting and/or FITS Services or any part thereof or necessary for the management, direction or control of the Hosting and/or FITS Services or any part thereof;
“Sub-contractor”	the third party with whom the Hosting Supplier enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents;
“Sub-contractor Credit Rating Threshold”	the Sub-contractor Credit Rating Thresholds as set out in Appendix 2 to schedule 7.4 (Financial Distress);
“Sub-contractor Financial Distress Event”	the occurrence of one or more of the events referred to in paragraph 9.1 of schedule 7.4 (Financial Distress);
“Subsequent Relevant Transfer”	has the meaning given to it in schedule 9.1 (Staff Transfers);
"Subsequent Transferring Employee"	has the meaning given to it in paragraph 1.1.5 of schedule 9.1 (Staff Transfers);
“Subsequent Transferring Employees”	has the meaning given to it in schedule 9.1 (Staff Transfers);
“Supplier Management Operations”	the forum described as such in the FITS Governance Framework;
“Supplier Test Policy”	has the meaning given to it in the Authority Test Strategy;
“Suppliers”	means FITS Suppliers;
“Suppliers’ Site”	Sites owned, controlled or occupied by the Suppliers which are used for the delivery by the Suppliers or their Sub-Contractors of End to End Services and/or FITS Services;
“Suppliers’ Solutions”	goods and services supplied by FITS Suppliers, as a response to business and technical challenges associated with the Authority’s business objectives;
"Supply Agreement"	means a Tower Service Agreement;

Term	Definition
“System Device”	any physical computing device used in the hosting and delivery of the FITS Services;
“System Integration Testing”	has the meaning given to it in the Authority Test Strategy;
“System Software”	the Software executed on System Devices used in the provision of FITS Services;
“Systems Management Tools”	has meaning given to it in schedule 8.1 (Definitions and Interpretation) of the MSA;
“Systems of Measurement”	the sources of data and calculations to be used in creating the monthly Service Level performance reports as set out as a Product Description to schedule 6.1 (Project Management);
“Systems of Measurement Referenced Document”	the detailed description of the sources of data, and calculations to be used in creating the monthly Service Level performance reports as set out as a Product Description to schedule 6.1 (Project Management);
“Tablet”	a portable computer contained in a single panel that uses a touch screen as its primary input device;
“Tapering Relief”	the tapering Bounded Mechanism as further described in paragraph 7.11 of schedule 7.1 (Charging and Invoicing);
“Technology Supplier”	Other FITS Suppliers and/or Other Authority Providers;
“Telephony Device”	any Device used in the delivery of Telephony Services;
“Telephony Services”	those services for the provision of telephony as set out in the Dependencies Register;
“Term”	the period commencing on the Effective Date and ending on the expiry of the Initial Term or the Extension Period or on earlier termination of this Agreement;
“Termination Assistance Notice”	has the meaning set out in paragraph 5.10 of schedule 8.5 (Exit Management);
“Termination Assistance Period”	the period specified in the Termination Assistance Notice in which the Hosting Supplier shall provide the Termination Hosting Services as may be extended pursuant to paragraph 5.11 of schedule 8.5 (Exit Management);
“Termination Notice”	a notice to terminate this Agreement or part of the Hosting Services and/or FITS Services either immediately or at a date specified in the notice;
“Termination Payments”	the payments described in paragraph 3.6 of schedule 7.2 (Payments on Termination);
“Termination Services”	the services and activities to be performed by the Hosting Supplier pursuant to the Exit Plan, including those activities listed in paragraph 5.15 of schedule 8.5 (Exit Management) and any other services required pursuant to the Termination Assistance Notice;
“Termination Threshold”	the applicable level at which the service performance gives rise to

Term	Definition
	a right of termination pursuant to clause 57.1.3.6 which is set out in Schedule 2.2 (Service Performance Management);
“Test”	has the meaning given to it in the Authority Test Strategy, covering any and all tests required to be carried out under this Agreement, pursuant to the Service Validation & Testing provisions of schedule 2.1 (Service Requirements) and schedule 2.3 (Standards), and “Tests” and “Testing” shall be construed accordingly;
“Test Asset”	has the meaning given to it in the Authority Test Strategy;
“Test Assurance”	has the meaning given to it in the Authority Test Strategy;
“Test Certificate”	the certificate materially in the form of the document contained in Appendix C to schedule 6.1 (Project Management) issued by the Authority when a Deliverable has satisfied its relevant Test Success Criteria satisfactorily;
“Test Environment”	has the meaning given to it in the Authority Test Strategy;
“Test Issue”	any variance or non-conformity of a Deliverable from its requirements as set out in the relevant Test Success Criteria;
“Test Item”	has the meaning given to it in the Authority Test Strategy;
“Test Manager”	has the meaning given to it in the Authority Test Strategy;
“Test Phase”	has the meaning given to it in the Authority Test Strategy;
“Test Plan”	a plan for the Testing of Deliverables and other agreed criteria related to the achievement of Milestones as described further in paragraph 5 of schedule 6.1 (Project Management);
“Test Report”	a report setting out the results of any Tests which shall include without limitation the information set out in paragraph 5.5 of schedule 6.1 (Project Management);
“Test Success Criteria”	the criteria developed in accordance with Part 3 of Schedule 6.1 (Project Management);
“Third Party Materials”	the Third Party Software together with the Documentation relating to the Third Party Software;
“Third Party Software”	software which is proprietary to any third party (other than an Affiliate of the Hosting Supplier) which is or will be used by the Hosting Supplier for the purposes of providing the Hosting Services and/or FITS Services, including the software specified as such in schedule 5.1 (Software);
“Threat”	threats include viruses, trojans, phishing and all other possible risks to FITS Services;
“Threshold Gain Margin”	the Forecast Gain Margin plus 0%. By way of example, if the Forecast Gain Margin is 10%, the Threshold Gain Margin would be 10%;
“TMO Services”	any services provided by Exiting Suppliers, Collaborating Suppliers, Other Authority Providers or FITS Suppliers provided

Term	Definition
	after the first Service Commencement Date for any of the Tower Services Agreements, but services provided prior to FMO;
“Tower Service Agreement”	a contract between the Authority and one of the FITS Suppliers;
“Tower Test Schedule”	the consolidated schedule (timings and dependencies) of all Transition-related Testing activities as set out in schedule 6.1 (Project Management);
“Tower Transition Management Groups”	as set out in paragraph 10.3.5 of schedule 6.1 (Project Management);
“Transferring Assets”	such assets as transferred to the Authority on termination or expiry of this Agreement and as specified in the Exit Plan;
“Transferring In Assets”	those assets which shall be transferred to the Hosting Supplier from an Exiting Supplier in accordance with the provisions of clause 10 (Transfer of Assets and Third Party Agreements) and schedule 6.3 (Asset Transfers);
“Transferring In Third Party Agreements”	agreements between the Authority or an Exiting Supplier and any third party which shall be transferred to the Hosting Supplier in accordance with the provisions of clause 10 (Transfer of Assets and Third Party Agreements) and schedule 6.3 (Asset Transfers);
“Transferring Out Assets”	those Assets which shall be transferred from the Hosting Supplier to a Replacement FITS Supplier (whether exit is because of expiry or termination) in accordance with the provisions of schedule 7.2 (Payments on Termination) and schedule 8.5 (Exit Management);
“Transferring Out Third Party Agreements”	agreements between the Hosting Supplier and any third party which shall be transferred to the Authority or to a Replacement FITS Supplier in accordance with the provisions of schedule 7.2 (Payments on Termination) and schedule 8.5 (Exit Management);
“Transformation Solutions”	where used, the transformation solutions set out in schedule 2.4 (Transformation);
“Transition”	the end-to-end processes, procedures, activities, Products, Documentation and Deliverables required to replace the services provided by the Exiting Suppliers with delivery of services by the FITS Suppliers under the Tower Service Agreements, and which involves but is not limited to the transfer of assets, personnel, premises, resources and work in progress;
“Transition Accelerated Ordering Process”	the process to support the accelerated ordering of goods or services during the End to End Transition;
“Transition Contingency Plan(s)”	describes the activities required to provide for any failure to maintain progress in Transition or meet any of the Milestones;
“Transition Deliverable”	any project document, item, feature or service associated with the Transition Services which is required to be provided by the Hosting Supplier in any plan, PID or Approval Criteria, as summarised in the Transition Deliverable Matrix managed by FTAF;
“Transition Deliverables”	as set out in Appendix B of schedule 6.1 (Project Management);

Term	Definition
Matrix	
“Transition Dependencies”	are the Delivery Dependencies;
“Transition Director”	a member of the Hosting Supplier’s personnel whose role is described in schedule 6.1 (Project Management);
“Transition Governance”	the governance process set out in schedule 6.1 (Project Management) and the FPMF;
“Transition Manager(s)”	managers who shall be responsible on a day-to-day basis for managing the Transition;
“Transition Mode of Operations”	the interim processes, procedures and ways of working to be utilised by the Exiting Suppliers and the FITS Suppliers, to enable the delivery of the FITS Services as part of the End to End Services during the transition period;
“Transition Models”	a repeatable way of dealing with the transition of FITS Services from one lifecycle status to the next;
“Transition Operational Control”	the Hosting Supplier function that shall be responsible for managing all Operational Changes that are related to transition activities;
“Transition Period”	the period of time beginning on the Effective Date of the SIAM Tower Service Agreement (3rd September 2013) and ending on Grand FMO;
“Transition Plans”	the FITS Programme Plan and the Levels 1 – 4 Plans;
“Transition Portfolio Plan”	is the FITS Programme Plan;
“Transition Portfolio Test Strategy”	the strategy produced to provide guidance and the approach to testing for the FITS Suppliers during the End to End Transition, as detailed in schedule 6.1 (Project Management);
“Transition Service Readiness Approach”	for measuring the transition service readiness developed in accordance with schedule 6.1 (Project Management);
“Transition Service Readiness Criteria”	the criteria set out in paragraphs 8.3.3(a)(i) to (v) inclusive of schedule 6.1 (Project Management);
“Transition Service Readiness Forum”	the Hosting Supplier’s main forum to demonstrate to the Authority that the Hosting Supplier has met the requirements set out in schedule 6.1 (Project Management) and that the Hosting Supplier is ready to deliver the Hosting Services;
“Transition Services”	the services described in schedule 6.1 (Project Management);
“Transition Table”	Table 1 set out in schedule 6.1 (Project Management);
“Transition Workstream(s)”	a project tasked with the Transition of a FITS Service or set of related FITS Services;
“Transition Workstream Manager(s)”	managers who shall be responsible for co-ordinating the detailed planning on each Transition Workstream;
“TSA Effective Date”	the date on which the Tower Service Agreement is signed by both

Term	Definition
	parties;
"TUPE"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 as amended from time to time;
"UK"	the United Kingdom;
"UK Expert Witness Register"	a register of Expert Witnesses located in the UK, normally operated by a commercial organisation, to enable legal professionals to locate experts with appropriate skills;
"UK GDPR"	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018;
"Unavailable" or "Unavailability"	has the same meaning as "Service Unavailability";
"United Kingdom Mainland"	means England, Scotland and Wales;
"Unused Access Device"	a device that provides access to any FITS Service through a network, but is no longer used;
"Unused Software"	software deployed to a device for consumption by a user but is no longer used;
"Updated Financial Model"	the Base Case Financial Model as updated pursuant to paragraph 5 of schedule 7.5 (Financial Model);
"Use"	<p>(a) with respect to the Standard Licence Terms and/or the Deposited Software, the right to load, execute, store, transmit, display and copy (for the purposes of loading, execution, storage, transmission or display);</p> <p>(b) with respect to the Enhanced Licence Terms, the Hosting Supplier's Background IPRs and/or Embedded Third Party IPRs, the right to load, execute, store, transmit, display, copy (for the purposes of loading, execution, storage, transmission or display), modify, adapt, enhance, reverse compile, decode, translate, publish (including on the ICT Environment), distribute or otherwise utilise;</p>
"User"	consumers of the End to End Services including but not limited to citizens and End Users;
"User Acceptance Testing"	has the meaning given to it in the Authority Test Strategy;
"User Administration"	the management of persons to use the FITS Services including their profile, credentials and rights of access;
"User Authentication"	the act of checking and confirming the true identity of a user prior to providing access to a FITS Service;
"VAT"	value added tax as provided for in the Value Added Tax Act 1994;
"VCS Bridge"	the Device and associated Software to connect multiple locations participating using video conferencing services (VCS) to a common video conference setting; providing both audio and real time visual interaction for the participants;

Term	Definition
“VCSE”	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
“Virus”	any “virus”, “malicious code” or “worm”, “Trojan Horse”, “trapdoor”, “Software Switch”, “time bomb” or “logic bomb”, “disabling code” or “disabling routines”, or “expiration dates” or spyware, but excluding any disabling codes, disabling routines or expiration dates which are notified in writing to and accepted by the Authority, as an integral part of software and where such notification includes details of trigger events which would activate such disabling codes, disabling routines or expiration dates, as these words are generally understood from time to time within the computer industry and any equivalent or similar corruptive mechanism;
“Vital Application”	a Business Application denoted as such within the Master Application List, but typically with the following characteristics: a Business Applications where the degradation or loss of the service would result in a major impact to the Authority’s productivity and / or reputation;
“Video Services”	as described in the Service Register;
“Video Services Terminal”	the Video Conferencing Devices comprising video screen, camera codec and audio ancillaries to enable high-definition collaboration services to court rooms, conference rooms and offices;
“Vital Services”	the services within the 'Vital Services' Band;
“REDACTED Background IPRs”	<p>(a) IPRs owned by REDACTED before the Effective Date, for example those subsisting in REDACTED standard development tools, program components or standard code used in computer programming or in physical or electronic media containing REDACTED Know-How or generic business methodologies;</p> <p>(b) IPRs created by REDACTED independently of this Agreement; and/or</p> <p>(c) The REDACTED Gold Build Security Configuration;</p>
“REDACTED Data Centre Facility”	the Sites REDACTED that are owned, or controlled, or occupied by the Data Centre Supplier which are used for the delivery by the Data Centre Supplier or its Sub-contractors for the provision of Data Centre Services;
REDACTED	REDACTED
“Vulnerability”	a weakness which allows an attacker to reduce a system's information assurance;
“Vulnerability Management”	the function responsible for the identification and possible reduction or elimination of any weakness that could be exploited by a Threat;

Term	Definition
“Vulnerability Management Team”	a team responsible for the implementation of counter measures against vulnerabilities;
“Vulnerability Resolution Plan”	a plan of actions agreed with the Authority to investigate, diagnose, resolve, and prevent future occurrences of a security vulnerability;
“WAN and LAN Services”	the services provided by the WAN and LAN Supplier;
“WAN and LAN Supplier”	a supplier under an agreement between the Authority and a provider of WAN and LAN services under the FITS Programme;
“Web Analytics”	the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimising web usage;
“Wide Area Network (WAN)”	a telecommunication network that covers a broad area (i.e. any network that links across metropolitan, regional, or national boundaries);
“WIP Deliverables”	the identified Deliverables as defined in the Project PID for the particular WIP activity;
“WIP Services”	those project services which were provided under the 2020 Hosting Agreement and which shall continue to be provided as part of the Hosting Services, subject to and in accordance with the terms of this Agreement, from and including the Effective Date, as more particularly described in Annex 1 to Schedule 6.2 (Work in Progress);
“Wireless LAN”	the IEEE family of standards for wireless networking, as defined by 802.11, and successors;
“Work In Progress”	any on-going, imminent or forecasted project, activity or initiative that may take place during End to End Transition;
“Work In Progress Control Procedure”	the Deliverable of the same name described in the relevant Product Description as set out in Appendix B to schedule 6.1 (Project Management);
“Work In Progress Solutions and Deliverables”	the FITS Supplier’s Solution and Plan to take over a Work In Progress from an Exiting Supplier;
“Working Day”	any day other than a Saturday, Sunday or public holiday in England and Wales;
“Workstream Plans”	a plan for the transition of a Work stream, as described in schedule 6.1 (Project Management).

End of Schedule