

Schedule 1

Definitions

“Accreditation”

means the process whereby the following aspects of an Information Storage/Processing Environment are articulated in a Risk Management & Accreditation Document Set (RMADS), and are formally reviewed and accepted by the relevant Accreditor and/or Senior Information Risk Owner (SIRO):

- (a) A description of the information storage/processing activity and the environment in which it takes place (what is stored/processed, when, where, how, by whom and for what purposes);
- (b) The native information security risks inherent to this activity;
- (c) The controls applied within the environment to mitigate these risks; and
- (d) The Residual Risks remaining after the application of controls (particularly where they exceed the SIRO's normal Risk Appetite),

and the terms "Accredit" and any other derivative term shall be construed accordingly;

“Accreditor”

means a HMG staff member who provides an end to end assurance and accreditation service for HMRC in accordance with HMRC and HMG Policy and standards and Good Industry Practice in respect of Information Management and Information Security. .

“Achieve” or “Achievement”

means, in respect of a Milestone, completion of the event or task represented by such Milestone;

“Additional Authority Customer”

Means any customer of the Authority who is not an Original Authority Customer and identified in a

	Services Order pursuant to Clause 10.3 and Schedule 11 (Services Order);
“ADR Notice”	shall have the meaning set out in Clause 61.3(b);
“Agreement”	means the Terms and Conditions, the Schedules and other attachments, as amended from time to time in accordance with this Agreement, and any other documents expressly identified in this document as forming part of the Agreement;
“Associate”	means 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;
“Assurance Tests”	means the testing to be carried out by the Supplier and the Authority in accordance with the Supplier’s Implementation Plan;
“Authorised Representative”	means any person authorised from time to time by the Authority or the Supplier to exercise any powers and/or undertake any activities of the Supplier or the Authority under and in accordance with the Agreement;
“Authority”	has the meaning set out at the head of this Agreement;
“Authority Audit Representatives”	means the Authority and its appointed contractors, the Authority’s external auditors and their appointed contractors and any other auditors (including internal auditors), regulators (including the National Audit Office), inspectors or contractors the Authority designates in writing from time to time;
“Authority Bank Account”	means any account from time to time maintained by the Authority or an Authority Customer with the Supplier and includes any sub-account of such an account;
“Authority Cause”	means any Default by the Authority or an Authority Customer, or its/their employees or authorised

persons including agents and contractors acting on its/their behalf, unless resulting from any act or omission by the Authority or Authority Customer, or its/their agents and contractors to which the Supplier or any Subcontractor has given its prior consent in writing;

“Authority Confidential Information”

means Confidential Information belonging to the Authority and/or any Authority Customer;

“Authority Customers”

means all of the Authority's customers (including all Government departments, executive agencies, non-Departmental public bodies and any other Crown Body or other public sector body or organisation to which the warranty set out in Clause 19.3(c) is applicable) for the benefit of which the Authority from time to time procures or agrees or arranges to provide or procure any of the Services including (a) the Original Authority Customers and (b) Additional Authority Customer;

“Authority Data”

means all data and information relating to the Authority and/or the Authority Customers (including Authority Personal Data) and the Services (in whatever form that information may exist) provided or made available to the Supplier by or on behalf of the Authority or any Authority Customer or produced or generated by the Supplier or any Subcontractor in connection with the provision of the Services;

“Authority Know How”

means all ideas, concepts, schemes, information, knowledge, techniques, methodology and anything else in the nature of know how of the Authority;

“Authority Mark”

means any trade mark or get-up, registered or unregistered, of the Authority or any Authority Customer;

“Authority Material”

means any Material owned by the Authority, including any Modifications to such Material from time to time, including Authority Software and Authority Data;

“Authority Personal Data”	means Authority Data which is personal data within the meaning of the DPA;
“Authority Relationship Manager”	has the meaning given in Clause 55;
“Authority Security Requirements”	the Authority’s requirements in respect of security as set out in Schedule 2 (Authority’s Service Requirements) and/or Schedule 9 (Information Security Assurance and Accreditation);
“Authority Sites”	means any and all of the freehold or leasehold sites owned or occupied by the Authority or any Authority Customer;
“Authority Software”	means Software and documentation (and any modifications to that Software) owned by the Authority or an Authority Customer and used or to be used in or for the purposes of receipt or use of the Services ;
“Authority Specific Change in Law”	means any Change in Law which affects solely or solely relates to the provision or operation of the Services or the Authority or any Authority Customer, but excluding any Change in Law that would have been reasonably foreseeable at the Effective Date by an experienced supplier performing services similar to the relevant Services on the basis of draft bills or proposals published in Government green or white papers or other Government departmental consultation papers, bills, draft statutory instruments or draft instruments or proposals published in the Official Journal of the European Union in each case published prior to the Effective Date;
“Authority’s Service Requirements”	means the Authority’s service requirements set out in Schedule 2 (as supplemented in accordance with any Services Orders pursuant to Schedule 11 (Services Order) and 12 (List of Original Authority Customers and their accompanying Services Orders));
“Benchmarking”	Shall have the meaning set out in paragraph 3.1 of

Schedule 4 (**Financial Obligations**);**“Business Continuity Plan”**

the plan relating to business continuity to be developed in accordance with Clause 17;

“CEDR”

means Centre for Effective Dispute Resolution;

“CESG”

means the UK National Technical Authority for Information Assurance, a part of Government Communications Headquarters (GCHQ), based at Hubble Road, Cheltenham;

“Change Communication”

means any Change Request or other communication sent or required to be sent pursuant to Schedule 8 (**Change Control Procedure**);

“Change Control Procedure”

means the procedure set out in Schedule 8 (**Change Control Procedure**) for dealing with Contract Changes;

“Change in Law”

means the coming into effect or repeal (without re-enactment or consolidation) of any Laws or any amendment or variation to any Laws, or any judgement of a relevant court of law which changes binding precedent in each case after the Effective Date;

“Change Manager”

means either the Authority's Change Manager or the Supplier's Change Manager, as the context so admits;

“Change of Control”

means that Control of the Supplier or the Supplier's parent undertaking is acquired by any entity or entities by way of a single transaction or series of related transactions;

“Claim”

shall have the meaning set out in Clause 45.1(a);

“Commencement Date”

means in relation to any Operational Services the date on which the Supplier begins providing those Operational Services to the Authority;

“Confidential Information”

means in relation to a Party, information that:

- (a) is by its nature confidential; and/or
- (b) is designated by that Party as confidential (whether by being Security Classified or otherwise); and/or
- (c) the other Party knows or ought to know is confidential;

and includes, to the extent that it is confidential:

- (i) information relating to the financial position or affairs, internal management or structure of the Party or its personnel, and strategies of the Party;
- (ii) the Agreement as limited by the operation of Clause 39.6;
- (iii) in the case of the Supplier, the Supplier Material; and
- (iv) in the case of Authority, the Authority Material, Services and the Authority Data;

“Continuing Term”

shall have the meaning set out in Clause 2(b);

“Contract Change”

means any change to this Agreement;

“Contract Change Request”

means a written (including email) request for a Contract Change which must be substantially in the form of Appendix 2 of Schedule 8 (**Change Control Procedure**);

“Control”

means the ultimate power to determine the direction of the management policies of such party, either directly or indirectly and whether through the ownership of voting securities, by contract or otherwise;

"Crown"	means 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, government and particular bodies and government agencies;
"Crown Body"	means any department, office or agency of the Crown;
"Default"	means any breach of the obligations of either Party (including a fundamental breach or breach of a fundamental term) or any default act, omission, negligence or statement of either Party, its employees, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Party is liable to the other;
"Delay"	means the period of time by which the implementation of the Services is delayed arising from a failure to Achieve a Milestone;
"Deliverables"	means all or any of the specific items or Services required to be provided by the Supplier pursuant to this Agreement and includes any designated Key Deliverables, any deliverables to be provided pursuant to a Contract Change and any upgrades and new releases;
"Disaster Recovery Plan"	the plan relating to Disaster Recovery as described in Clause 17;
"Dispute Resolution Procedure"	means the procedure for the resolution of disputes specified in Clause 61;
"DOTAS"	means the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue and Customs of any specified notifiable

arrangements or proposals and to provide prescribed information on those arrangements or proposals within 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.

“DPA”	means the Data Protection Act 1998 (as amended or replaced from time to time);
“EEA”	means European Economic Area;
“Effective Date”	means the date of this Agreement;
“Emergency Change”	means any Contract Change which the Parties agree needs to be dealt with urgently;
“Escalation Procedure”	shall mean the procedure set out in paragraph 2.2.4 of Schedule 6 (Governance and Co-operation);
“Ethical Walls”	means a system of effective internal measures to ensure that information relating to one part of the Supplier’s business is withheld from, and shall not be used in, another part of the Supplier’s business;
“Exit Manager”	has the meaning set out in Paragraph 3.1 of Appendix 2 of Schedule 10 (Exit Management);
“Exit Management Plan”	means the plan to be agreed between the Supplier and the Authority that shall set out each Party’s obligations in detail in order to ensure a smooth and efficient transfer of the Services to a Successor Supplier;
“Exit Period”	means the period beginning on the earlier of the following dates: (i) the Supplier being notified in writing by the

Authority of the Authority's intention to commence a Procurement Process in respect of the Services; or

(ii) the Supplier receives notice of termination;

and ending on the Services Transfer Date;

"FOIA"

means the Freedom of Information Act 2000 together with any subordinate legislation made under that Act from time to time, guidance and/or codes of practice issued by the Information Commissioner or relevant Crown Body in relation to such Act;

"FOIA Notice"

means a decision notice, enforcement notice and/or an information notice;

"Force Majeure Event"

means any cause directly affecting the performance by a party of its obligations under this Agreement arising from acts, events or omissions beyond its reasonable control, including:

- (a) fire, flood, earthquake, elements of nature or act of God; or
- (b) war, riot, civil disorder, rebellion, terrorism or revolution;

"Future Services"

means services which are outside the scope of the Authority's Service Requirements and ordered in accordance with Clause 11;

"General Anti Abuse Rule"

means (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 including to avoid national insurance contributions.

"General Change in Law"

means any Change in Law which is not an Authority Specific Change in Law;

"Good Industry Practice"

means at any time the exercise of that degree of skill, diligence, prudence and foresight which would

reasonably and ordinarily be expected at such a time from a highly skilled and experienced provider of services similar to the Services seeking in good faith to comply with its contractual obligations and complying with all relevant Laws;

“Halifax Abuse Principle”

means the principle explained in the CJEU Case C-255/02 Halifax and others.

“Hardware”

means all hardware used to provide the Operational Services, including desktop hardware, servers, network components peripheral devices (including printers and scanners) mobile computing devices (including laptops and PDAs)), cabling, ducting and cabinets;

“HMG Security Policy Framework”

means the standards, best practice guidelines and approaches that are required to protect UK Government assets (people, information and infrastructure) as published from time to time by the Cabinet Office (currently at: <http://www.gov.uk/government/publications/security-policy-framework>), and which is split into tiers which vary in the level of detail they articulate and thus their intended audience as follows:

Tier 1: Overarching Security Statement (high-level intent)

Tier 2: Core Security Principles

Tier 3: Key Security Policies, which identify a number of minimum mandatory outcomes (mandatory requirements)

Tier 4: technical standards, supplementary policy and best practice guidance;

“Implementation”

means the implementation and commencement of Operational Services;

“Implementation Board”

means the board (comprising of representatives from both Parties) appointed by the Authority to monitor the Implementation Services;

“Implementation Services”

means the Services necessary to achieve

Implementation;

“Independent Assessor”

means the representative of a suitably qualified professional benchmarking organisation;

“Indexation”

means in respect of any period the application of a percentage change equal to the percentage change in the Consumer Price Index published by the Office of National Statistics over the same period;

“Information Risk Appetite”

means Risk Appetite in the specific context of information security as articulated by each Department's Senior Information Risk Owner (SIRO) using a number of different taxonomies, but most commonly using the HM Treasury scale *“Thinking About Risk”* and/or identifying the maximum risk level resulting from a CESG Information Assurance Standard No 1 (IS1) technical risk assessment that they will tolerate without approving a detailed risk acceptance case for each specific risk;

“Information Storage/Processing Environment”

means the collection of all those components that enable the storage and/or processing of information in support of a given business purpose and which may include technology components, people, processes and physical premises;

“Initial Term”

shall have the meaning set out in Clause 2(a);

“Insolvency Event”

shall have the meaning set out in Clause 48.1(b);

“Intellectual Property Rights” or “IPRs”

any current and future intellectual property rights, including:

- (a) copyrights, trade marks, trade names, domain names, rights in logos and get-up, inventions, confidential information, trade secrets and know-how including commercial know-how, design rights, rights in inventions, patents, utility models, semi-conductor topographies and rights in databases; and
- (b) all intangible rights and privileges of a nature

similar, analogous or allied to any of the above;

in every case in any part of the world and whether or not registered, including in relation to the above:

- (c) all granted registrations and all applications for registration;
- (d) all renewals, reversions or extensions;
- (e) the right to sue for damages for past infringement; and
- (f) all forms of protection of a similar nature which may subsist anywhere in the world;

“Internal Audit Plan”

means a document that lays out the Supplier's proposed Internal Audit Programme for a future period of time (usually a 12 month 'audit year', where the start and end of the audit year is defined consistently across the Supplier's business in calendar date terms);

“Internal Audit Programme”

means a series of activities that are conducted by the Supplier to provide ongoing internal challenge, validation and assurance over whether its documented processes are being followed by its staff and Subcontractor(s), and that the controls (security controls and controls of other types) that it believes to have in place are operating effectively and providing for a degree of independence between those staff carrying out the audit and the business area being audited in order to ensure that the audit is both impartial and objective;

“ISMS”

Means an information security management system as defined by ISO/IEC 27001; being that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security, as agreed by the Parties and directly reflecting the scope of the Services;

“Key Deliverable”

means, in relation to each part of the Operational Services whose implementation and commencement is separately provided for in the Overall Implementation Plan set out in Schedule 5, the Implementation of those Operational Services;

“Laws”

means:

- (a) any statute, regulation, by law, ordinance or subordinate legislation in force from time to time to which a Party hereto is subject;
- (b) the common law as applicable to the Parties hereto from time to time;
- (c) any binding court order, judgement or decree given in respect of a Party hereto;
- (d) any applicable mandatory industry code, or standard enforceable by law; and
- (e) any applicable direction, rule or order that is binding on a Party hereto and that is made or given by any regulatory body having jurisdiction over a Party or any of that Party's assets, resources or business;

“Losses”

means all losses, liabilities, damages, costs and expenses (including reasonable legal fees on a solicitor/client basis and reasonable disbursements and reasonable costs of investigation, litigation, settlement, judgement, interest and penalties);

“Material”

means any Software, firmware, database, documented methodology or process, documentation or other material in whatever form, including, any reports, specifications, processes, designs and configuration, business rules or requirements, system architecture documents and designs, user manuals, user guides, web pages, operations manuals, training materials and instructions;

“Measurement Window”

means the period over which the services or any part of them shall be measured, as specified in Schedule 3 (**Service Levels**);

“Milestone Date”

means in relation to each Key Deliverable a date specifically identified in the Supplier’s Implementation Plan (which date shall be no later than the date identified in the Overall Implementation Plan as set out in Schedule 5) by which that Key Deliverable is to be completed in accordance with the terms of this Agreement;

“Model Procedure”

shall have the meaning set out in Clause 61.3(a);

“Native Risk(s)”

means the risks inherent to a given information storage and/or processing activity, based on factors such as: the sensitivity and quantity of information being stored/processed, the attractiveness of that information to unauthorised persons, the nature of the processing activity that the information enables or supports, and the attributes of the environment within which the information is being stored or processed and which are risks that have not been subject to any risk mitigation through the application of controls;

“Notice” or “Notify”

means a notice given in accordance with Clause 59;

“Occasion of Tax Non Compliance”

means

(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found to be incorrect as a result of:

(i) a Relevant Tax Authority successfully challenging the 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;

(ii) the failure of an avoidance scheme which the 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

(b) the Supplier's tax affairs give rise on or after 1 April 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;

"Operational Services"

means all of the Services apart from the Implementation Services;

"Ordinary Course of Business"

means either:

(a) any acts, omissions or conduct which is consistent in all respects with the prevailing pattern, or course of conduct, or management used by the Supplier in the provision of the Services or undertaken in order to comply with the applicable obligations under the Agreement; or

(b) acts, omissions or conduct which a well managed company would undertake (assuming that such company is acting in a prudent and reasonable manner) in relation to the provision of the Services or in order to comply with all applicable obligations under the Agreement,

whichever imposes the higher standard;

"Original Authority Customer"

means those Authority Customers who will transfer

			from the Outgoing Supplier to the Supplier on the Commencement Date, set out in Schedule 12 (List of Authority Customers and their accompanying Services Orders);
“Other Expedited Contract Change”			means any Contract Change which the Parties agree to expedite in accordance with paragraph 9 of Appendix 1 to Schedule 8 (Change Control Procedure);
“Outgoing Supplier”			means any party including the Authority or any other supplier providing services to the Authority or any Authority Customer prior to the Commencement Date which are the same as or substantially similar to the Services;
“Outline Exit Management Plan”			means the minimum provisions that will be included in any Exit Management Plan, as listed in Appendix 5 of Schedule 10 (Exit Management);
“Overall Implementation Plan”			has the meaning given in Clause 7.2;
“Party”			means a party to this Agreement and “Parties” means both parties to this Agreement;
“Personnel”			means employees, officers and individuals contracted to the Supplier and involved to any extent in the provision of the Services;
“Procurement Process”			means the process by which the Authority may seek tenders for the provision of any of the Services;
“Publicity Material”			shall have the meaning set out in Clause 73.1(b);
“Relevant Tax Authority”			means HM Revenue and Customs, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established;
“Regulator”			means the Financial Conduct Authority and/or the Prudential Regulation Authority or any successor to the Financial Conduct Authority or the

	Prudential Regulation Authority;
“Remedial Plan”	shall have the meaning set out in Clause 48.2;
“Remedial Plan Notice”	shall have the meaning set out in Clause 48.2;
“Remedial Plan Process”	shall have the meaning set out in Clause 48.2;
“Residual Risk”	means a Native Risk that has been subject to mitigation through the application of controls and typically has a lower probability of manifestation, and/or a lesser impact should they manifest, than the Native Risk to which it corresponds as a result of the application of controls (provided that a given Native Risk and its corresponding Residual Risk may be identical, if there are no controls in place to mitigate that risk or if the controls applied are ineffective at mitigating it);
“Risk Appetite”	means the amount of risk a Department of Government is ordinarily prepared to tolerate in the delivery of its Departmental objectives and which is often articulated using the scale identified in HM Treasury’s <i>“Thinking About Risk”</i> guidance, which can be found at: http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/d/tar_practitioners_guide.pdf ;
“Risk Management & Accreditation Document Set (RMADS)”	means a portfolio of documentation that describes the risk considerations applicable to a given Information Storage/Processing Environment and which builds the case for the Accreditation of the environment to which it relates by demonstrating that the applicable risks have been captured, quantified and mitigated in accordance with the relevant Senior Information Risk Owner (SIRO)’s Information Risk Appetite and which is reviewed by the relevant Accreditor in order to decide whether or not to Accredite the environment to which it relates, and is maintained in order to periodically re-Accredite the environment (usually upon a significant change being made to the Information Storage/Processing

	Environment, with significance being at the sole discretion of the relevant Accreditor; or, in any event, not less than annually);
“Schedule”	means each of Schedules 1 to 12 of this Agreement;
“Security Classified”	shall have the meaning as set out in the HMG Security Policy Framework;
“Security Event”	means an observation, which may or may not take the form of an entry in a security log or other audit log, that indicates that a Security Incident has, or may have, taken place (which may in itself have a low probability of indicating that a Security Incident has occurred while correlation between multiple Security Events may represent a strong predictor that a Security Incident has in fact occurred);
“Security Exit Management Plan”	means the plan prepared by the Supplier pursuant to paragraph 3.5 of Schedule 9 (Information Security Assurance and Accreditation);
“Security Improvement Plan”	means an agreed programme of activities to minimise the risks applicable to a given Information Storage/Processing Environment, and/or to provide the necessary level of assurance that the implemented controls are operating effectively, in which the identified activities should be proportionate, prioritised and time-bound;
“Security Incident”	means, in accordance with the Authority’s Security Requirements in Schedule 2 (Authority’s Service Requirements) and the Security Policy, the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Sites, the Supplier Systems and/or any ICT (Information and Communication Technology), information or data (including the Confidential Information and the Authority Data) used by the Authority

and/or the Supplier in connection with this Agreement;

(b) the loss and/or unauthorised disclosure of any information or data, any malicious act that results in the unavailability of any information or data, and/or the failure to keep the integrity of any information or data, including in all cases the Confidential Information and the Authority Data and including in all cases any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement; and/or

any instances of economic crime or other types of fraud perpetrated by, using or through the Services;

“Security Management Plan”

means the plan prepared by the Supplier pursuant to paragraph 3 of Schedule 9 (**Information Security Assurance and Accreditation**);

“Security Policy”

means the Authority's security policy as attached as Appendix 1 to Schedule 9 (**Information Security Assurance and Accreditation**) and as updated from time to time;

“Security Tests”

means any and all such audits, inspections or other tests (practical or otherwise) of the Supplier's policies, process or Supplier Systems as are necessary for the Authority to gain comfort that the Supplier's declared system(s) of governance and control, and/or other mitigations of the risks applicable to the environment in which the Authority's data is processed, are adequate and effective;

“Security Working Group”

means the joint Authority/Supplier forum described in paragraph 10 of Schedule 9 (**Information Security Assurance and Accreditation**);

“Senior Information Risk Owner (SIRO)”

means the HMG staff member ultimately accountable for the information security risks

applicable to a given information storage/processing activity or environment;

“Senior Stakeholders”

means the group (comprising of representatives from both Parties) appointed by the Authority to monitor partnering issues, delivery of Services and any issues that are unresolved by the Implementation Board and/or the Supplier Review Board;

“Service Charges”

means the charges paid or payable to the Supplier by the Authority in accordance with Schedule 4 (**Financial Obligations**) for the supply of the Services;

“Service Credits”

means, in relation to the relevant Service Levels as set out in Schedule 3 (**Service Levels**), credits which are payable by the Supplier where due to a Default by the Supplier the Services have failed to meet those Service Levels;

“Service Level”

means the service levels set out in Schedule 3 (**Service Levels**);

“Service Level Default”

means a failure by the Supplier to perform the Services in accordance with or to the standard required by the Service Levels;

“Services”

means all those services required by the Authority to be provided by the Supplier pursuant to this Agreement and particularly Schedule 2 (**Authority’s Service Requirements**);

“Services Order”

means a services order issued by the Authority to the Supplier on the *pro forma* set out in Schedule 11, pursuant to which the Supplier shall supply Services to an Original Authority Customer or an Additional Authority Customer;

“Services Transfer Date”	means the date that any of the Services are transferred from the Supplier to a Successor Supplier and the Successor Supplier takes full responsibility for them;
“Services Transfer Plan”	means the final form exit and transfer arrangements setting out the timetable and scope of required activities for transferring any of the Services to the Successor Supplier based upon the relevant provisions of the Exit Management Plan;
“Software”	means any computer program or programming (including source code (except in the case of third party software licensed in object code form only), object code and executable code) and an item of Software includes, without limitation, any software Tools or object libraries embedded in that Software and all Materials relating to that Software and/or its design, development, operation, support or maintenance, and in the case of third party software, includes any Materials made available by the third party to the Supplier under or in relation to the licence for that third party software;
“Staff Transfer”	means the transfer of staff pursuant to the Transfer of Undertakings (Protection of Employment) Regulations 2006;
“Subcontractor”	means any subcontractor or agent or partner of the Supplier (including but not limited to any Associate of the Supplier and excluding any payment industry infrastructure used by banks generally in the provision of banking services), appointed by the Supplier for the purpose of providing the Services (or part of the Services) on behalf of the Supplier to the Authority and/or Authority Customers;
“Successor Supplier”	means any party or parties (including the Authority, or a new third party supplier or suppliers) that the Authority nominates to provide services equivalent to or replacing any or all of the Services;

“Supplier”	has the meaning set out at the head of this Agreement;
“Supplier Group Company”	means the Supplier and any undertaking which is, from time to time, a subsidiary undertaking of the Supplier, a parent undertaking of the Supplier or a subsidiary undertaking of a parent undertaking of the Supplier, as those terms are construed in accordance with Section 1162 of the Companies Act 2006, as amended;
“Supplier Relationship Manager”	has the meaning given in Clause 55;
“Supplier Review Board”	means the board (comprising of representatives from both Parties) appointed by the Authority to monitor the Operational Services and any Termination Assistance;
“Supplier System(s)”	means any and all information communications technology (ICT) Hardware, Software or infrastructure (or any other technological components) that are owned or operated by the Supplier or any Subcontractor(s) and that will store or process Authority Data and/or Authority Confidential Information or otherwise contribute to the Supplier's delivery of the Services, including any and all audit, back-up, restoration, redundant ('failover'), contingency or other components that comprise the Supplier's means of ensuring business continuity in the Supplier's delivery of Services to the Authority, in addition to any primary systems that such capabilities assure, support or replace;
“Supplier’s Confidential Information”	means Confidential Information belonging to the Supplier or any Subcontractor;

“Supplier’s Implementation Plan”	has the meaning given in Clause 7.2;
“Supplier’s Sites”	means the freehold or leasehold sites (or any of them) owned or occupied by the Supplier and used by or on behalf of the Supplier to perform the Services;
“Supplier’s Software”	means Software and documentation (and any modifications to that Software) owned by the Supplier and used by or on behalf of the Supplier to perform the Services;
“Supplier’s Solution”	means the Supplier's specification for the Services set out in Schedule 2;
“Surviving Clauses”	shall have the meaning set out in Clause 52;
“Term”	means the Initial Term and any Continuing Term;
“Termination Assistance”	means the assistance to be provided by the Supplier to the Authority in order to effect the smooth handover of part or all of the Services from the Supplier to a Successor Supplier (or to the Authority) in accordance with Schedule 10 (Exit Management);
“Termination Date”	means the effective date of termination of the Agreement as specified in a notice of termination, or the expiry date of the Agreement;
“Termination Notice”	means a notice to terminate this Agreement or part of the Services either immediately or at a date specified in the notice;
“Termination Transfer Employee”	means each employee included in the list of Personnel who will or are expected to transfer to a Successor Supplier provided in accordance with Appendix 4 of Schedule 10 (Exit Management);
“Terms and Conditions”	means the terms and conditions of this Agreement, excluding the Schedules and any Annexes;

“Tools”	means any program used for software development, testing or maintenance, data search or analysis including related methodologies, processes and know-how;
“TUPE” or “Transfer Regulations”	means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (as amended from time to time) or any legislation enacted to replace those regulations;
UKAS	means the United Kingdom Accreditation Service, the sole national accreditation body recognised by Government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services;
“Use”	means the right to utilise including copying, modifying and further developing any Materials, communicating, making available and distributing the same internally;
“VAT”	means value added tax;
“Working Day”	means Monday to Friday (excluding Bank Holidays in England & Wales, Northern Ireland or in Scotland as applicable).