Bevan Brittan

Dated **2023**

(1) THE DIRECTOR OF SAVINGS

and

(2) SOPRA STERIA LIMITED

AGREEMENT
relating to CUSTOMER CONTACT AND OPERATIONS

Toronto Square – 7th Floor | Toronto Street | Leeds LS1 2HJ
T 0370 194 1000 F 0370 194 5465

Fleet Place House | 2 Fleet Place | Holborn Viaduct | London EC4M 7RF
T 0370 194 1000 F 0370 194 7800

Kings Orchard | 1 Queen Street | Bristol BS2 0HQ
T 0370 194 1000 F 0370 194 1001

Interchange Place | Edmund Street | Birmingham B3 2TA
T 0370 194 1000 F 0370 194 5001

www.bevanbrittan.com

Contents

Item		Page
SECTION A – PRELIMINARIES		3
1	DEFINITIONS AND INTERPRETATION	3
2	DUE DILIGENCE	5
3	WARRANTIES	6
SECTION B – THE SERVICES		8
4	TERM	8
5	SERVICES	9
6	IMPLEMENTATION	14
7	PERFORMANCE INDICATORS	14
8	SERVICES IMPROVEMENT	17
9	EQUIPMENT AND MAINTENANCE	17
SECTION C – PAYMENT, TAXATION AND VALUE FOR MONEY PROVISIONS		17
10	FINANCIAL AND TAXATION MATTERS	17
SECTION D – CONTRACT GOVERNANCE		19
11	GOVERNANCE	19
12	RECORDS, REPORTS, AUDITS & OPEN BOOK DATA	19
13	CHANGE	20
SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN		21
14	SUPPLIER PERSONNEL	21
15	SUPPLY CHAIN RIGHTS AND PROTECTIONS	24
SECTION F – INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY		30
16	INTELLECTUAL PROPERTY RIGHTS	30
17	TRANSFER AND LICENCES GRANTED BY THE SUPPLIER	31
18	ESCROW	34
19	LICENCES GRANTED BY THE DIRECTOR	34
20	IPRS INDEMNITY	36
21	OPEN SOURCE PUBLICATION	37
22	DIRECTOR DATA AND SECURITY REQUIREMENTS	37
23	CONFIDENTIALITY	38
24	TRANSPARENCY AND FREEDOM OF INFORMATION	40
25	PROTECTION OF PERSONAL DATA	41
26	PUBLICITY AND BRANDING	46
SECTION G – LIABILITY, INDEMNITIES AND INSURANCE		46
27	LIMITATIONS ON LIABILITY	46
28	INSURANCE	49
SECTION H – REMEDIES AND RELIEF		49
29	RECTIFICATION PLAN PROCESS	49

30 NOT USED 52
31 REMEDIAL ADVISER 52
32 STEP-IN RIGHTS 55
33 DIRECTOR CAUSE 56
34 FORCE MAJEURE 58
SECTION I – TERMINATION AND EXIT MANAGEMENT 59
35 TERMINATION RIGHTS 59
36 CONSEQUENCES OF EXPIRY OR TERMINATION 60
SECTION J – MISCELLANEOUS AND GOVERNING LAW 62
37 COMPLIANCE 62
38 ASSIGNMENT AND NOVATION 62
39 WAIVER AND CUMULATIVE REMEDIES 63
40 RELATIONSHIP OF THE PARTIES 63
41 PREVENTION OF FRAUD AND BRIBERY 63
42 CONFLICTS OF INTEREST 64
43 SEVERANCE 66
44 FURTHER ASSURANCES 66
45 ENTIRE AGREEMENT 66
46 THIRD PARTY RIGHTS 66
47 NOTICES 67
48 DISPUTES 68
49 GOVERNING LAW AND JURISDICTION 68

SCHEDULES

Schedule 1 - Definitions
Schedule 2.1 – Service Description
Schedule 2.2 – Performance Levels
Schedule 2.3 - Standards
Schedule 2.4 – Security Management
Schedule 2.5 – Insurance Requirements
Schedule 3 – Director Responsibilities
Schedule 4.1 – Supplier Solution
Schedule 4.2 Commercially Sensitive Information
Schedule 4.3 Key Sub-contractors
Schedule 4.4 – Third Party Contracts
Schedule 5.1 - Software
Schedule 5.2 Trade Marks
Schedule 6.1 Implementation Plan
Schedule 6.2 – Testing Procedures
Schedule 7.1 – Charging and Invoicing
Schedule 7.2 – Payments on Termination
Schedule 7.3 - Benchmarking
Schedule 7.4 – Financial Distress
Schedule 7.5 - Financial Reports, Audit and Risk
Schedule 7.6 – Regulatory Compliance and Financial Crime
Schedule 8.1 - Governance
Schedule 8.2 - Change Control Procedure

Schedule 8.3 – Dispute Resolution Procedure
Schedule 8.4 – Reports and Records Provisions
Schedule 8.5 – Exit Management
Schedule 8.6 – Service Continuity Plan and Corporate Resolution Planning
Schedule 8.7 – Conduct of Claims
Schedule 8.8 – Continuous Improvement
Schedule 9.1 – Staff Transfer
Schedule 9.2 – Key Personnel
Schedule 10 - Guarantee
Schedule 11 – Processing Personal Data
Schedule 12 – Collaboration Agreement

THIS AGREEMENT is made on 2023

BETWEEN:

(1) **THE DIRECTOR OF SAVINGS** as agent of the Crown ("**Director"**); and

(2) **SOPRA STERIA LIMITED** a company registered in England and Wales under company number 04077975 whose registered office is at Three Cherry Trees Lane, Hemel Hempstead, Hertfordshire, HP2 7AH ("**Supplier"**)

(each a "**Party**" and together the "**Parties**").

INTRODUCTION

(A) The Director is an Executive Agency of the Chancellor of the Exchequer. It is one of the UK's largest retail savings organisations with twenty five (25) million customers and more than £202,000,000,000 (two hundred and two billion pounds) of funds under management, best known for Premium Bonds but also offering a wide range of other savings products. The Director raises cost-effective financing for the Government, by offering a range of secure retail financial savings products, as an alternative to raising funds on the wholesale market.

(B) The Director is seeking to establish a set of contracts, of which this is one, to deliver an end to end solution to manage its sales processing and customer service functions along with IT and Infrastructure Services.

(C) This Agreement is intended to deliver Customer contact and operations to improve Customer experiences that establish a seamless 'Assisted Digital' service to Customers and automate processing where possible. The Service shall include provision of a Contact Centre and operational sites, as well as non-digitised processing, printing and mailing services. The Supplier shall also provide complaints management and the appropriate Supplier Personnel to undertake all of the relevant Services.

(D) On 29th April 2022 the Director advertised on the e-tendering portal Find a Tender Service (reference 2022/S 000-011240), inviting prospective suppliers to submit proposals for the Contact Centre and associated services.

(E) The Supplier is a leading provider of consulting, digital services and software development and has experience in customer contact and operations.

(F) On the basis of the Supplier's response to the advertisement and a subsequent tender process, the Director selected the Supplier as its preferred supplier.

(G) Following negotiations, the Parties have agreed to contract with each other in accordance with the terms and conditions set out below.

(H) The Director currently provides services to other government departments through its B2B Services offering known as NS&I Government Payment Services (NS&I GPS). NS&I GPS offers modern, secure and highly competitive banking and payments services available to all government departments, agencies and other public sector organisations to meet current and future needs. Whilst the Director does not require the delivery of B2B Services at the Effective Date, there is potential for B2B Services to expand during the lifetime of this Agreement and the Find a Tender Service notice is intended to allow for the delivery of customer contact and operations to support B2B Services/NS&I GPS activities, leveraging the Services procured under this Agreement.

IT IS AGREED as follows:

SECTION A – PRELIMINARIES

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless otherwise provided or the context otherwise requires, capitalised expressions shall have the meanings set out in Schedule 1 (*Definitions*) or the relevant Schedule in which that capitalised expression appears.

1.2 In this Agreement, unless the context otherwise requires:

1.2.1 the singular includes the plural and vice versa;

1.2.2 reference to a gender includes the other gender and the neuter;

1.2.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;

1.2.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.2.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation";

1.2.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.2.7 the headings are for ease of reference only and shall not affect the interpretation or construction of this Agreement;

1.2.8 unless otherwise provided and save for references in Annexes of Schedule 5.1 (*Software*) and in Schedule 10 (*Guarantee*), references to Clauses and Schedules are references to the clauses and schedules of this Agreement and references in any Schedule to Paragraphs, Parts and Annexes are, unless otherwise provided, references to the paragraphs, parts and annexes of the Schedule or the Part of the Schedule in which the references appear; and

1.2.9 references to this Agreement are references to this Agreement as amended from time to time.

1.3 Where a standard, policy or document is referred to in this Agreement by reference to a hyperlink, then if the hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Director and the Parties shall update this Agreement with a reference to the replacement hyperlink.

1.4 Reference to a "relevant governance board" shall mean a governance board set out in Schedule 8.1 (*Governance*) whose terms of reference covers the subject matter identified or, if none, the governance board specified by the Director from time to time.

1.5 Time is not of the essence of any obligation of the Director under this Agreement and may not be made of the essence by service of notice.

1.6 If there is any conflict between the Clauses and the Schedules and/or any Annexes to the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

1.6.1 the Clauses and Schedule 1 (*Definitions*);

1.6.2 Schedules 2.1 (*Services Description*) and 2.2 (*Performance Levels*) and their Annexes;

1.6.3 any other Schedules and their Annexes (other than Schedule 4.1 (*Supplier Solution*) and its Annexes); and

1.6.4 Schedule 4.1 (*Supplier Solution*) and its Annexes (if any).

1.7 The Schedules and their Annexes form part of this Agreement.

1.8 In entering into this Agreement the Director is acting as part of the Crown.

1.9 Prompt and expedited performance of this Agreement is important to the Director. In all cases therefore where the Provider is obliged to take action, provide notice or complete a task under this Agreement, then, where there is no specific statement as to timing, there shall be implied an obligation to do so promptly. This is without prejudice to any specific time limits set out in this Agreement.

2 DUE DILIGENCE

2.1 The Supplier acknowledges that, subject to the Allowable Assumptions:

2.1.1 the Director has delivered or made available to the Supplier all of the information and documents that the Supplier considers necessary or relevant for the performance of its obligations under this Agreement;

2.1.2 it has made its own enquiries to satisfy itself as to the accuracy and adequacy of the Due Diligence Information;

2.1.3 it has satisfied itself (whether by inspection or having raised all relevant due diligence questions with the Director before the Effective Date) of all relevant details relating to:

(a) the Director Requirements;

(b) the suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Effective Date) future Operating Environment;

(c) the operating processes and procedures and the working methods of the Director;

(d) the ownership, functionality, capacity, condition and suitability for use in the Services of the Director Assets; and

(e) the existing contracts (including any licences, support, maintenance and other agreements relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Agreement and/or which the Supplier will require the benefit of for the provision of the Services; and

2.1.4 it has advised the Director in writing of:

(a) each aspect, if any, of the Operating Environment that is not suitable for the provision of the Services;

(b) the actions needed to remedy each such unsuitable aspect; and

(c) a timetable for and, to the extent that such costs are to be payable to the Supplier, the costs of those actions,

and such actions, timetable and costs are fully reflected in this Agreement, including the Services Description and/or Director Responsibilities as applicable.

2.2 Further the Director may from time to time share requirements and/or proposed solutions in respect of Relevant Third Party Supplier contracts, when they become available whether through the Change

Control Procedure or otherwise, with the Supplier. The Supplier, shall within ten (10) Working Days of receiving the requirements and/or proposed solutions and subject always to the Supplier complying with Clause 42 (*Conflicts of Interest*), shall notify the Director of:

2.2.1 any issues with the requirements and/or proposed solutions;

2.2.2 any impact on the Supplier or the Services arising from the requirements and/or proposed solutions, including any additional activities of the Supplier in supporting the implementation of the Relevant Third Party Supplier solution which could not have been foreseen prior to the requirements and any associated impact on the Supplier's obligations under Schedule 6.1 (*Implementation Plan*); and

2.2.3 any Dependencies, other than those already documented in this Agreement and/or the Collaboration Agreement, the Supplier will have on an appointed Relevant Third Party Supplier.

The Supplier shall also provide such support as the Director may require during the procurement of Relevant Third Party Supplier contracts, including requests to update the Supplier responses to the requirements. If the support required exceeds five (5) person days' effort then the Director shall raise a request for the effort in excess of five (5) person days as an Additional Service in accordance with Clause 5.11.

2.3 The Supplier shall not be excused from the performance of any of its obligations under this Agreement on the grounds of, nor (subject to Clause 2.4), shall the Supplier be entitled to recover any additional costs or charges, arising as a result of:

2.3.1 any unsuitable aspects of the Operating Environment;

2.3.2 any misinterpretation of the Director Requirements;

2.3.3 any failure by the Supplier to satisfy itself as to the accuracy and/or adequacy of the Due Diligence Information; and/or

2.3.4 any failure to respond or otherwise identify issues, impacts or Dependencies in accordance with Clause 2.2.

2.4 The Parties shall comply with the provisions of Paragraph 6 of Part 3 of Schedule 7.1 (*Charges and Invoicing*) in relation to the verification of any Allowable Assumptions.

3 WARRANTIES

3.1 The Director represents and warrants that:

3.1.1 it has full capacity and authority to enter into and to perform this Agreement;

3.1.2 this Agreement is executed by its duly authorised representative;

3.1.3 there are no actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, threatened against it that might affect its ability to perform its obligations under this Agreement; and

3.1.4 its obligations under this Agreement constitute its legal, valid and binding obligations, enforceable in accordance with their respective terms subject to applicable bankruptcy, reorganisation, insolvency, moratorium or similar Laws affecting creditors' rights generally and subject, as to enforceability, to equitable principles of general application (regardless of whether enforcement is sought in a proceeding in equity or law).

3.2 The Supplier represents and warrants that:

3.2.1 it is validly incorporated, organised and subsisting in accordance with the Laws of its place of incorporation;

3.2.2 it has full capacity and authority to enter into and to perform this Agreement;

3.2.3 this Agreement is executed by its duly authorised representative;

3.2.4 it has all necessary consents and regulatory approvals to enter into this Agreement;

3.2.5 it has notified the Director in writing of any actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, any threatened against it or any of its Affiliates that might affect its ability to perform its obligations under this Agreement;

3.2.6 its execution, delivery and performance of its obligations under this Agreement will not constitute a breach of any Law or obligation applicable to it and will not cause or result in a default under any agreement by which it is bound;

3.2.7 its obligations under this Agreement constitute its legal, valid and binding obligations, enforceable in accordance with their respective terms subject to applicable bankruptcy, reorganisation, insolvency, moratorium or similar Laws affecting creditors' rights generally and subject, as to enforceability, to equitable principles of general application (regardless of whether enforcement is sought in a proceeding in equity or law);

3.2.8 all written statements and representations in any written submissions made by the Supplier as part of the procurement process, including without limitation its response to the selection questionnaire, its final tender (ISFT) and any other documents submitted remain true and accurate except to the extent that such statements and representations have been superseded or varied by this Agreement or to the extent that the Supplier has otherwise disclosed to the Director in writing prior to the date of this Agreement;

3.2.9 it has notified the Director in writing of any Occasions of Tax Non-Compliance and any litigation in which it is involved that is in connection with any Occasion of Tax Non-Compliance;

3.2.10 it has all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier Background IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Director which are necessary for the performance of the Supplier's obligations under this Agreement and/or the receipt of the Services by the Director;

3.2.11 the Contract Inception Report is a true and accurate reflection of the Costs and Supplier Profit Margin forecast by the Supplier and the Supplier does not have any other internal financial model in relation to the Services inconsistent with the Financial Model;

3.2.12 it is not subject to any contractual obligation, including in relation to any other contract it may have with the Director compliance with which is likely to have a material adverse effect on its ability to perform its obligations under this Agreement;

3.2.13 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue; and

3.2.14 within the previous twelve (12) months, no Financial Distress Events have occurred or are subsisting (or any events that would be deemed to be Financial Distress Events under this Agreement had this Agreement been in force) and there are currently no matters that it is aware of that could cause a Financial Distress Event to occur or subsist.

3.3 The representations and warranties set out in Clause 3.2 shall be deemed to be repeated by the Supplier on the Effective Date (if later than the date of signature of this Agreement) by reference to the facts then existing.

3.4 Each of the representations and warranties set out in Clauses 3.1 and 3.2 shall be construed as a separate representation and warranty and shall not be limited or restricted by reference to, or inference from, the terms of any other representation, warranty or any other undertaking in this Agreement.

3.5 If at any time a Party becomes aware that a representation or warranty given by it under Clause 3.1 or 3.2 has been breached, is untrue or is misleading, it shall immediately notify the other Party of the relevant occurrence in sufficient detail to enable the other Party to make an accurate assessment of the situation.

3.6 For the avoidance of doubt, the fact that any provision within this Agreement is expressed as a warranty shall not preclude any right of termination which the Director may have in respect of breach of that provision by the Supplier.

3.7 Except as expressly stated in this Agreement, all warranties and conditions whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by Law.

SECTION B – THE SERVICES

4 TERM

4.1 This Agreement shall:

4.1.1 come into force on the Effective Date, save for Clauses 1 (*Definitions and Interpretation*), 3 (*Warranties*), 4 (*Term*), 23 (*Confidentiality)*, 24 (*Transparency and Freedom of Information*), 26 (*Publicity and Branding*), 27 (*Limitations on Liability*), 39 (*Waiver and Cumulative Remedies*), 40 (*Relationship of the Parties*), 43 (*Severance*), 45 (*Entire Agreement)*, 46 (*Third Party Rights*), 47 (*Notices*), 48 (*Disputes*) and 49 (*Governing Law and Jurisdiction*), which shall be binding and enforceable as between the Parties from the date of signature; and

4.1.2 unless terminated at an earlier date by operation of Law or in accordance with Clause 35 (*Termination Rights*), terminate:

(a) at the end of the Initial Term; or

(b) if the Director elects to extend the Initial Term by giving the Supplier at least sixty (60) Working Days' notice before the end of the Initial Term, at the end of the Extension Period.

Condition Precedent

4.2 Save for Clauses 1 (*Definitions and Interpretation*), 3 (*Warranties*), 4 (*Term*), 23 (*Confidentiality*), 24 (*Transparency and Freedom of Information*), 26 (*Publicity and Branding*), 27 (*Limitations on Liability*), 39 (*Waiver and Cumulative Remedies*), 40 (*Relationship of the Parties*), 43 (*Severance*), 45 (*Entire Agreement*), 46 (*Third Party Rights*), 47 (*Notices*), 48 (*Disputes*) and 49 (*Governing Law and Jurisdiction)*, this Agreement is conditional upon the valid execution and delivery to the Director of:

4.2.1 the Guarantee; and

4.2.2 the Collaboration Agreement.

(the "**Condition Precedent**").

The Director may in its sole discretion at any time agree to waive compliance with the Condition Precedent by giving the Supplier notice in writing.

4.3 The Supplier shall satisfy, or procure the satisfaction of, the Condition Precedent as soon as possible. In the event that the Condition Precedent is not satisfied within twenty (20) Working Days after the date of this Agreement (or such extended timescales as the Director may, at its sole discretion, notify the Supplier in writing of) then, unless the Condition Precedent is waived by the Director in accordance with Clause 4.2:

4.3.1 this Agreement shall automatically cease and shall not come into effect; and

4.3.2 the Director shall have no obligation to pay any compensation to the Supplier as a result of such cessation.

4.4 The Supplier shall consult with the Director in relation to the steps it takes to satisfy the condition set out in Clause 4.2 and shall keep the Director fully informed of its progress in satisfying the condition and of any circumstances which are likely to result in the condition not being satisfied by the date set out in Clause 4.3.

5 SERVICES

Standard of Services

5.1 The Supplier shall provide:

5.1.1 the Implementation Services (or part thereof) from (and including) the relevant Implementation Services Commencement Date(s); and

5.1.2 the Operational Services (or part thereof) in each case from (and including) the relevant Operational Service Commencement Date.

5.2 The Supplier shall ensure that the Services:

5.2.1 comply in all respects with the Services Description; and

5.2.2 are supplied in accordance with the Supplier Solution and the provisions of this Agreement; and

5.2.3 are supplied in a joined up way with the Relevant Third Party Suppliers so as to deliver a customer focused end to end solution.

5.3 The Supplier shall perform its obligations under this Agreement and the Collaboration Agreement, including in relation to the supply of the Services in accordance with:

5.3.1 all applicable Law, including, but not limited to those identified in Schedule 7.6 (*Regulatory Compliance and Financial Crime*) and any other regulatory or compliance obligations for which the Supplier is subject to or responsible for compliance with;

5.3.2 Good Industry Practice;

5.3.3 the Standards;

5.3.4 the Baseline Security Requirements;

5.3.5 the Quality Plans; and

5.3.6 the Supplier's own established procedures and practices to the extent the same do not conflict with the requirements of Clauses 5.3.1 to 5.3.5.

5.4 In the event that the Supplier becomes aware of any inconsistency between the requirements of Clauses 5.3.1 to 5.3.5, the Supplier shall immediately notify the Director Representative in writing of

such inconsistency and the Director Representative shall, as soon as practicable, notify the Supplier which requirement the Supplier shall comply with.

5.5 The Supplier shall:

5.5.1 deliver the Services using efficient business processes and ways of working having regard to the Director's obligation to ensure value for money;

5.5.2 provide sufficient resources with the appropriate technical expertise to:

(a) make up, run and operate the Development Pool in order to deliver ongoing Change pursuant to Schedule 8.2 (*Change Control Procedure*);

(b) supply the Deliverables; and

(c) provide the Services in accordance with this Agreement;

5.5.3 strive to deliver excellent Customer service and deliver the Services in a manner which preserves and, where possible, enhances the Director's brand and reputation as a leading brand in the market;

5.5.4 continue to modernise the Services in accordance with Good Industry Practice and input into the Continuous Improvement Plan; and

5.5.5 provide operational capacity and capabilities that can cope with short, medium and long-term demand fluctuations.

Supplier covenants

5.6 The Supplier shall:

5.6.1 at all times provide the Assets necessary to enable it to provide the Services and allocate sufficient resources with the appropriate technical expertise to supply the Deliverables and to provide the Services in accordance with this Agreement;

5.6.2 save to the extent that obtaining and maintaining the same are Director Responsibilities and subject to Clause 13 (*Change*), obtain, and maintain throughout the duration of this Agreement, all the consents, approvals, licences and permissions (statutory, regulatory, contractual or otherwise) it may require and which are necessary for the provision of the Services;

5.6.3 ensure that:

(a) it shall continue to have all necessary rights in and to the Licensed Software, the Third Party IPRs, the Supplier Background IPRs and any other materials made available by the Supplier (and/or any Sub-contractor) to the Director which are necessary for the performance of the Supplier's obligations under this Agreement and/or the receipt of the Services by the Director;

(b) the release of any new Software or upgrade to any Software complies with the interface requirements in the Services Description and (except in relation to new Software or upgrades which are released to address Malicious Software or to comply with the requirements of Schedule 2.4 (*Security Management*)) shall notify the Director three (3) months before the release of any new Software or Upgrade. The Supplier shall ensure any release is in compliance with all security, audit, testing and other applicable procedures;

(c) subject to the requirements set out in Schedule 2.4 (*Security Management*), all Software including Upgrades, Updates and New Releases used by or on behalf of

the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

(d) any products or services recommended or otherwise specified by the Supplier for use by the Director in conjunction with the Deliverables and/or the Services shall enable the Deliverables and/or Services to meet the Director Requirements; and

(e) the Supplier System and Assets used in the performance of the Services will be free of all encumbrances (except as agreed in writing with the Director);

5.6.4 minimise any disruption to the Services, the IT Environment, Relevant Third Party Supplier services and/or the Director's operations when carrying out its obligations under this Agreement;

5.6.5 ensure that any Documentation and training provided by the Supplier to the Director are comprehensive, accurate and prepared in accordance with Good Industry Practice and maintain a complete and up to date description of the Services and the solution to deliver them, which shall be available to the Director at any point during the term within two (2) Working Days of the Director's request;

5.6.6 co-operate with the Relevant Third Party Suppliers and provide reasonable information (including any Documentation), advice and assistance in connection with the Services to any Relevant Third Party Supplier to enable such Relevant Third Party Supplier to create and maintain technical or organisational interfaces with the Services and, on the expiry or termination of this Agreement for any reason, to enable the timely transition of the Services (or any of them) to the Director and/or to any Replacement Supplier;

5.6.7 co-operate with and support the Director in delivering a customer focused end to end solution;

5.6.8 to the extent it is legally able to do so, hold on trust for the sole benefit of the Director, all warranties and indemnities provided by third parties or any Sub-contractor in respect of any Deliverables and/or the Services and, where any such warranties are held on trust, at its cost enforce such warranties in accordance with any reasonable directions that the Director may notify from time to time to the Supplier;

5.6.9 unless it is unable to do so, assign to the Director on the Director's written request and at the cost of the Supplier any such warranties and/or indemnities as are referred to in Clause 5.6.8;

5.6.10 provide the Director with such assistance as the Director may reasonably require during the Term in respect of the supply of the Services;

5.6.11 gather, collate and provide such information and co-operation as the Director may reasonably request for the purposes of ascertaining the Supplier's compliance with its obligations under this Agreement;

5.6.12 notify the Director in writing as soon as reasonably possible and in any event within one (1) month of any change of Control taking place;

5.6.13 notify the Director in writing within ten (10) Working Days of their occurrence, of any actions, suits or proceedings or regulatory investigations before any court or administrative body or arbitration tribunal pending or, to its knowledge, threatened against it that might affect its ability to perform its obligations under this Agreement;

5.6.14 ensure that neither it, nor any of its Affiliates, embarrasses the Director or otherwise brings the Director into disrepute, including by engaging in any act or omission in relation to this Agreement which is reasonably likely to diminish the trust that the public places in the Director; and

5.6.15 manage closure or termination of Services to take account of the Director's disposal requirements, including recycling and scope for re-use, and all applicable Standards.

5.7 An obligation on the Supplier to do, or to refrain from doing, any act or thing shall include an obligation upon the Supplier to procure that all Sub-contractors and Supplier Personnel also do, or refrain from doing, such act or thing.

5.8 Without prejudice to Clauses 20.2 and 20.3 (*IPRs Indemnity*) and any other rights and remedies of the Director howsoever arising, the Supplier shall:

5.8.1 remedy any breach of its obligations in Clauses 5.6.2 to 5.6.4 inclusive within no more than three (3) Working Days of becoming aware of the breach or being notified of the breach by the Director where practicable or within such other time period as may be agreed with the Director (at all times taking into account the nature of the breach that has occurred);

5.8.2 remedy any breach of its obligations in Clause 5.6.1 and Clauses 5.6.5 to 5.6.11 inclusive within twenty (20) Working Days of becoming aware of the breach or being notified of the breach by the Director; and

5.8.3 meet all the costs of, and incidental to, the performance of such remedial work,

and any failure of the Supplier to comply with its obligations under Clause 5.8.1 or Clause 5.8.2 within the specified or agreed timeframe shall constitute a Notifiable Default.

Specially Written Software warranty

5.9 Without prejudice to Clauses 5.6 (*Supplier Covenants*) and 5.8 (*Services*) and any other rights and remedies of the Director howsoever arising, the Supplier warrants to the Director that all components of the Specially Written Software shall:

5.9.1 be free from material design and programming errors;

5.9.2 perform in all material respects in accordance with the relevant specifications contained in the Supplier Solution and Documentation; and

5.9.3 not infringe any Intellectual Property Rights.

Continuing obligation to provide the Services

5.10 The Supplier shall continue to perform all of its obligations under this Agreement and shall not suspend the supply of the Services, notwithstanding:

5.10.1 any withholding of the Service Charges by the Director pursuant to Clause 7.2.4(b) (*Performance Failures*);

5.10.2 the existence of an unresolved Dispute; and/or

5.10.3 any failure by the Director to pay any Charges,

unless the Supplier is entitled to terminate this Agreement under Clause 35.3 (*Termination by the Supplier*) for failure to pay undisputed Charges.

Additional Services

5.11 The Director may require the Supplier to provide any or all of the Additional Services at any time by giving notice to the Supplier in writing. The Supplier acknowledges that the Director is not obliged to take any Additional Services from the Supplier and that nothing shall prevent the Director from receiving services that are the same as or similar to the Additional Services from any third party.

5.12 If a Change Request is required to be submitted, the Supplier shall, as part of the Impact Assessment provided by the Supplier in relation to such Change Request, provide details of the impact (if any) that the proposed Change will have on the relevant Additional Services. Notwithstanding Paragraph 3.2 of Schedule 8.2 (*Change Control Procedure*), the Supplier shall also provide details of whether such Change Request can be delivered as a DevOps Change through the Development Pool.

5.13 Following receipt of the Director's notice pursuant to Clause 5.11:

5.13.1 the Parties shall document the inclusion of the relevant Additional Services within the Services in accordance with the Change Control Procedure, modified to reflect the fact that the terms and conditions on which the Supplier shall provide the relevant Additional Services have already been agreed;

5.13.2 the Supplier shall implement and Test the relevant Additional Services in accordance with the Additional Services Implementation Plan;

5.13.3 any additional charges for the Additional Services shall be in accordance with and incorporated in the Charges as specified in Paragraph 3 of Part 2 of Schedule 7.1 (*Charges and Invoicing*); and

5.13.4 the Supplier shall, from the date agreed in the Additional Services Implementation Plan (or, if later, the date of Achievement of any Milestones associated with the commencement of the relevant Additional Services (if any)), provide the relevant Additional Services to meet or exceed the applicable Target Performance Level in respect of all Performance Indicators applicable to the Additional Services as set out in Annex 1 of Schedule 2.2 (*Performance Levels*).

5.14 Any Change relating to Additional Services shall incorporate the principles of this Clause 5.14:

5.14.1 the Additional Services shall be delivered under the terms of this Agreement and in accordance with the Service Description;

5.14.2 the Anticipated Contract Life Profit Margin under the Agreement must not increase as a consequence of the incorporation of the Additional Services unless otherwise agreed between the Parties;

5.14.3 subject to Clause 5.14.2, there must be no alteration of the allocation of risk between the Parties in respect of the existing Services;

5.14.4 the associated marginal cost and Charges for the delivery of the Services shall be used as the basis of the costs and charges for the Additional Services;

5.14.5 there shall be no double recovery of costs in respect of Charges for an Additional Service. Where costs are fully or partially recovered through the Charges, such costs shall be excluded from any charges for Additional Services; and

5.14.6 unless otherwise agreed by the Director no Termination Payment or Compensation Payment shall be paid to the Supplier on the expiry or termination of the Additional Services.

Power of attorney

5.15 By way of security for the performance of its obligations under Clauses 5.6.8 and 5.6.9 (*Supplier covenants*) the Supplier hereby irrevocably appoints the Director as its agent and attorney to act with full power and authority in the Supplier's name and on its behalf to do all such acts and execute all such documents as may be necessary or desirable to enforce any such warranties and/or effect any such assignment as are referred to in such Clauses and to delegate one or more of the powers conferred on it by this Clause 5.15 (other than the power to delegate) to officer(s) appointed for that purpose by the Director and may vary or revoke such delegation at any time.

Director Responsibilities

5.16 The Director shall comply with its responsibilities set out in Schedule 3 (*Director Responsibilities*).

6 IMPLEMENTATION

Quality Plans

6.1 The Supplier shall develop, within twenty (20) Working Days of the Effective Date, quality plans that ensure that all aspects of the Services are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").

6.2 The Supplier shall obtain the Director Representative's written approval of the Quality Plans before implementing them, which approval shall not be unreasonably withheld or delayed. The Supplier acknowledges and accepts that the Director's approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Services are provided to the standard required by this Agreement.

6.3 Following the approval by the Director of the Quality Plans:

6.3.1 the Supplier shall design and deliver all Deliverables in accordance with the Quality Plans and to align with the Director's overarching Quality Plans for the End to End Services; and

6.3.2 any Changes to the Quality Plans shall be agreed in accordance with the Change Control Procedure.

Implementation Plan and Delays

6.4 The Parties shall comply with the provisions of Schedule 6.1 (*Implementation Plan*) in relation to the agreement and maintenance of the Detailed Implementation Plan.

6.5 The Supplier shall:

6.5.1 comply with the Implementation Plan(s); and

6.5.2 ensure that each Milestone is Achieved on or before its Milestone Date.

6.6 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay:

6.6.1 it shall:

(a) notify the Director in accordance with Clause 29.1 (*Rectification Plan Process*);

(b) comply with the Rectification Plan Process in order to address the impact of the Delay or anticipated Delay; and

(c) use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

Testing and Achievement of Milestones

6.7 The Parties shall comply with the provisions of Schedule 6.2 (*Testing Procedures*) in relation to the procedures to determine whether a Milestone or Test has been Achieved.

7 PERFORMANCE INDICATORS

7.1 The Supplier shall:

7.1.1 provide the Operational Services (or part thereof) in such a manner so as to meet or exceed the Target Performance Level for each Performance Indicator from the relevant Operational Services Commencement Date; and

7.1.2 comply with the provisions of Schedule 2.2 (*Performance Levels*) in relation to the monitoring and reporting on its performance against the Performance Indicators.

Performance Failures

7.2 If in any Service Period:

7.2.1 a KPI Failure occurs, Service Credits shall be deducted from the Service Charges in accordance with Paragraph 2 of Part 3 of Schedule 7.1 (*Charges and Invoicing*);

7.2.2 a Material KPI Failure occurs, the Supplier shall comply with the Rectification Plan Process (in addition to Service Credits accruing in accordance with Clause 7.2.1);

7.2.3 a PI Failure occurs, the Supplier shall notify the Director of the action (if any) it will take to rectify the PI Failure and/or to prevent the PI Failure from recurring; and/or

7.2.4 a Material PI Failure occurs:

(a) the Supplier shall comply with the Rectification Plan Process; and

(b) the Director may withhold a proportionate amount of the Service Charges in accordance with the process set out in Clause 10.7 (*Set-off and Withholding*) until the relevant Material PI Failure is rectified to the reasonable satisfaction of the Director, at which point the Director shall pay the amount withheld.

Unacceptable KPI Failure

7.3 If in any Service Period an Unacceptable KPI Failure occurs:

7.3.1 the Director shall (subject to the Service Credit Cap set out in Clause 27.4.3 (*Financial and other limits*)) be entitled to withhold and retain as compensation for the Unacceptable KPI Failure a sum equal to the Service Charges which would otherwise have been due to the Supplier in respect of that impacted element of the Operational Services within the Service Period (such sum being "**Compensation for Unacceptable KPI Failure**"); and

7.3.2 if the Director withholds and retains such Compensation for Unacceptable KPI Failure, any Service Points and Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue,

provided that the operation of this Clause 7.3 shall be without prejudice to any right which the Director may have to terminate this Agreement and/or to claim damages from the Supplier as a result of such Unacceptable KPI Failure.

7.4 The Supplier:

7.4.1 agrees that the application of Clause 7.3 is commercially justifiable where an Unacceptable KPI Failure occurs; and

7.4.2 acknowledges that it has taken legal advice on the application of Clause 7.3 and has had the opportunity to price for that risk when calculating the Service Charges.

Critical Performance Failure

7.5 If a Critical Performance Failure occurs, the Director may exercise its rights to terminate this Agreement in whole or in part pursuant to Clause 35.1 or 35.2 (*Termination by the Director*).

Changes to Performance Indicators and Service Credits

7.6 Subject to Clause 7.6.3, not more than once in each Contract Year (save where Clause 7.7 or Clause 7.8 applies) the Director may, on giving the Supplier at least three (3) months' notice:

7.6.1 change the weighting that applies in respect of one or more specific Key Performance Indicators;

7.6.2 change and/or introduce new Key Performance Indicators and/or Performance Indicators but subject always to the Director Requirements; and/or

7.6.3 following the final Operational Services Commencement Date the Director may change and/or introduce new Key Performance Indicators and/or Performance Indicators where the existing Key Performance Indicators and/or Performance Indicators are deemed by the Director to be redundant or less relevant taking into account changes arising from transformation to the future operating model of the Services and/or changes in the method of delivery and/or solution used to deliver the Services; and/or

7.6.4 convert one or more:

(a) Key Performance Indicators into a Performance Indicator; and/or

(b) Performance Indicators into a Key Performance Indicator (in which event the Director shall also set out in the notice details of what will constitute a Minor KPI Failure, a Serious KPI Failure and a Severe KPI Failure for the new Key Performance Indicator).

7.7 In circumstances where the Target Performance Level of a Subsidiary Performance Indicator has not been met in any three (3) months in any rolling period of twelve (12) months, then the Subsidiary Performance Indicator shall in the month following the third (3rd) month of failure be converted to a Key Performance Indicator with the relevant Service Point weightings as set out in Schedule 2.2 (*Performance Levels*). The Director shall be entitled to apply Service Credits to this Key Performance Indicator in addition to those applying to the other Key Performance Indicators at that time without any dilution. Thereafter, where the Service Provider satisfies the Target Performance Level of such a Key Performance Indicator (that had been converted from the Subsidiary Performance Indicator) in three (3) consecutive months then the Key Performance Indicator in question shall be converted back to a Subsidiary Performance Indicator.

7.8 Schedule 2.2 (*Performance Levels*) identifies several Performance Indicators that will only be effective upon the carrying out by the Supplier of certain Services and which do not, at the Effective Date, contain relevant Target Performance Levels. The Parties acknowledge that upon the occurrence of the relevant Milestone or other date or event as set out in Schedule 2.2 (*Performance Levels*) for each of those Key Performance Indicators to become effective, the Director shall, at least thirty (30) days before such Performance Indicators becoming effective, confirm the Target Performance Levels and other details of what will constitute a Minor KPI Failure, a Serious KPI Failure and a Severe KPI Failure or similar based on its consideration of the baseline data provided by the Supplier in the relevant Performance Monitoring Report. Upon each of the Performance Indicators becoming effective (on the occurrence of the events as set out in Schedule 2.2) the Director shall be entitled to apply Service Credits to such Performance Indicators in addition to those applying to the other Key Performance Indicators at that time without any dilution of the Service Points.

7.9 If the Director wishes to change or amend the Key Performance Indicators or the Performance Indictors at a time other than as set out in Clause 7.6.1 to Clause 7.9 inclusive, it may do so but this will be treated as a Change.

7.10 The Supplier shall not be entitled to object to any changes made by the Director under Clause 7.6, 7.7, 7.8, 7.9 or increase the Service Charges as a result of such changes provided that:

7.10.1 the total number of Key Performance Indicators does not exceed fifty (50);

7.10.2 the principal purpose of the change is to reflect changes in the Director's business requirements and/or priorities and/or to reflect demand or the nature of the Director's business following completion of the Implementation Services and/ or to reflect changing industry standards or performance improvement including improved collaboration pursuant to the Collaboration Agreement; and

7.10.3 there is no change to the Service Credit Cap.

8 SERVICES IMPROVEMENT

8.1 The Parties shall comply with the provisions of Schedule 8.8 (*Continuous Improvement*) in relation to the improvement of any or all of the Services.

9 EQUIPMENT AND MAINTENANCE

Supplier Equipment

9.1 The Supplier shall be solely responsible for the cost of carriage of Supplier Equipment to any Sites including its off-loading, removal of all packaging and all other associated costs. Likewise on termination or expiry of this Agreement, the Supplier shall be responsible for the removal and safe disposal of all relevant Supplier Equipment from any Sites, including that of the Relevant Third Party Suppliers and the Director Premises and including the cost of packing, carriage and making good the Sites following removal, and taking account of any sustainability requirements, including safe removal of data and recycling requirements.

9.2 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Director shall be liable for loss of or damage to any of the Supplier's property located on Director Premises which is due to the negligent act or omission of the Director.

9.3 Subject to any express provision of the Service Continuity Plan to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Agreement, including the Target Performance Levels.

Maintenance

9.4 The Supplier shall create and maintain a rolling schedule of planned maintenance to the IT Environment (the "**Maintenance Schedule**") which shall be agreed with the Director. The Supplier shall ensure that it takes into consideration the Maintenance Schedule of Relevant Third Party Suppliers. Once the Maintenance Schedule has been agreed with the Director Representative, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule and ensure that all such Permitted Maintenance continues to meet and satisfy all security, audit, testing and other applicable standards and procedures.

9.5 Notwithstanding Clause 9.4, where the Director, acting reasonably, requires Permitted Maintenance to be delayed it shall notify the Supplier and the parties shall agree a revised date for the delayed Permitted Maintenance.

9.6 The Supplier shall give as much notice as is reasonably practicable to the Director Representative prior to carrying out any Emergency Maintenance.

9.7 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the IT Environment or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to have no impact on the IT Environment or Services.

SECTION C – PAYMENT, TAXATION AND VALUE FOR MONEY PROVISIONS

10 FINANCIAL AND TAXATION MATTERS

Charges and Invoicing

10.1 In consideration of the Supplier carrying out its obligations under this Agreement, including the provision of the Services, the Director shall pay the Charges to the Supplier in accordance with the pricing and payment profile and the invoicing procedure specified in Schedule 7.1 (*Charges and Invoicing*).

10.2 Except as otherwise provided, each Party shall each bear its own costs and expenses incurred in respect of compliance with its obligations under Clauses: 6.7 (*Testing and Achievement of Milestones*), 12 (*Records, Reports, Audits & Open Book Data*), 24 (*Transparency and Freedom of Information*), 25 (*Protection of Personal Data*) and, to the extent specified therein, Clause 31 (*Remedial Adviser*) and Clause 32 (*Step-In Rights*).

10.3 If the Director fails to pay any undisputed Charges properly invoiced under this Agreement, the Supplier shall have the right to charge interest on the overdue amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

VAT

10.4 The Charges are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Director following delivery of a valid VAT invoice.

10.5 The Supplier shall indemnify the Director on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Director at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 10.5 shall be paid in cleared funds by the Supplier to the Director not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Director.

Set-off and Withholding

10.6 The Director may set off any amount owed by the Supplier to the Crown or any part of the Crown (including the Director) against any amount due to the Supplier under this Agreement or under any other agreement between the Supplier and the Director.

10.7 If the Director wishes to:

10.7.1 set off any amount owed by the Supplier to the Crown or any part of the Crown (including the Director) against any amount due to the Supplier pursuant to Clause 10.6; or

10.7.2 exercise its right pursuant to Clause 7.2.4(b) (*Performance Failures*) to withhold payment of a proportion of the Service Charges,

it shall give notice to the Supplier within thirty (30) days of receipt of the relevant invoice, setting out the Director's reasons for withholding or retaining the relevant Charges.

Benchmarking

10.8 The Parties shall comply with the provisions of Schedule 7.3 (*Benchmarking*) in relation to the benchmarking of any or all of the Services.

Financial Distress

10.9 The Parties shall comply with the provisions of Schedule 7.4 (*Financial Distress*) in relation to the assessment of the financial standing of the Supplier and other specified entities and the consequences of a change to that financial standing.

Promoting Tax Compliance

10.10 If, at any point during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:

10.10.1 notify the Director in writing of such fact within five (5) Working Days of its occurrence; and

10.10.2 promptly provide to the Director:

(a) details of the steps which the Supplier is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Occasion of Tax Non-Compliance as the Director may reasonably require.

Compensation and Goodwill Payments

10.11 The Supplier hereby indemnifies the Director against all Compensation and Goodwill Payments arising from the Services in accordance with Paragraph 4 of Part 3 of Schedule 7.1 (*Charges and Invoicing*) and which are paid or payable by the Director (or by the Supplier on its behalf).

10.12 If in any month a Compensation and Goodwill Payment is made by the Supplier in accordance with Paragraph 3 of Part 3 of Schedule 7.1 (*Charges and Invoicing*) and it is determined to be attributable to a Relevant Third Party Supplier, the Supplier shall be entitled to recover from the Director the relevant sums in accordance with Paragraph 3.6 of Part 3 of Schedule 7.1 (*Charges and Invoicing*).

10.13 The Supplier shall comply with the Rectification Plan Process in order to address the underlying cause giving rise to a Compensation and Goodwill Payment attributable to the Services in accordance with Paragraph 3.5 of Part 3 of Schedule 7.1 (*Charges and Invoicing*).

SECTION D – CONTRACT GOVERNANCE

11 GOVERNANCE

11.1 The Parties shall comply with the provisions of Schedule 8.1 (*Governance*) in relation to the management and governance of this Agreement.

Representatives

11.2 Each Party shall have a representative for the duration of this Agreement who shall have the authority to act on behalf of their respective Party on the matters set out in, or in connection with, this Agreement.

11.3 The initial Supplier Representative shall be the person named as such in Schedule 9.2 (*Key Personnel*). Any change to the Supplier Representative shall be agreed in accordance with Clause 14 (*Supplier Personnel*).

11.4 The Director shall notify the Supplier of the identity of the initial Director Representative within five (5) Working Days of the Effective Date. The Director may, by written notice to the Supplier, revoke or amend the authority of the Director Representative or appoint a new Director Representative.

12 RECORDS, REPORTS, AUDITS & OPEN BOOK DATA

12.1 The Supplier shall comply with the provisions of:

12.1.1 Schedule 8.4 (*Reports and Records Provisions*) in relation to the maintenance and retention of Records;

12.1.2 Part 1 of Schedule 7.5 (*Financial Reports, Audit and Risk*) in relation to the maintenance of Open Book Data;

12.1.3 Part 4 of Schedule 7.5 (*Financial Reports, Audit and Risk*) in relation to the implementation of a risk management framework; and

12.1.4 Schedule 7.6 (*Regulatory Compliance and Financial Crime*) in relation to delivery of Services in accordance with relevant regulatory and compliance frameworks and in relation to the Supplier's fraud and financial crime investigation and recovery and engagement with other financial institutions.

12.2 The Parties shall comply with the provisions of:

12.2.1 Part 2 of Schedule 7.5 (*Financial Reports, Audit, Risk and Compliance*) in relation to the provision of the Financial Reports; and

12.2.2 Part 3 of Schedule 7.5 (*Financial Reports, Audit, Risk and Compliance*) in relation to the exercise of the Audit Rights by the Director or any Audit Agents.

13 CHANGE

Change Control Procedure

13.1 Any requirement for a Change shall be subject to the Change Control Procedure.

Change in Law

13.2 The Supplier shall neither be relieved of its obligations to supply the Services in accordance with the terms and conditions of this Agreement nor be entitled to an increase in the Charges as the result of:

13.2.1 a General Change in Law; or

13.2.2 a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Effective Date.

13.3 For the purposes of Clause 13.2, a Change in Law which affects Relevant Third Party Suppliers or Sub-Contractors (either of the Supplier, Director or Relevant Third Party Suppliers) which requires a change to the Services or the Agreement shall be deemed a General Change in Law.

13.4 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in Clause 13.2.2), the Supplier shall:

13.4.1 notify the Director as soon as reasonably practicable of the likely effects of that change, including:

(a) whether any Change is required to the Services, the Charges or this Agreement; and

(b) whether any relief from compliance with the Supplier's obligations is required, including any obligation to Achieve a Milestone and/or to meet the Target Performance Levels; and

13.4.2 provide the Director with evidence:

(a) that the Supplier has minimised any increase in costs or maximised any reduction in costs, including in respect of the costs of its Sub-contractors;

(b) as to how the Specific Change in Law:

(i) has affected the cost of providing the Services; and

(ii) prevents the Supplier from meeting its obligations, including any obligation to Achieve a Milestone and/or to meet the Target Performance Levels; and

(c) demonstrating that any expenditure that has been avoided, for example which would have been required under the provisions of Clause 8 (*Services Improvement*), has been taken into account in amending the Charges.

13.5 Any variation in the Charges or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in Clause 13.2.2) shall be implemented in accordance with the Change Control Procedure.

SECTION E – SUPPLIER PERSONNEL AND SUPPLY CHAIN

14 SUPPLIER PERSONNEL

14.1 The Supplier shall:

14.1.1 provide in advance of any admission to Director Premises a list of the names of all Supplier Personnel requiring such admission, specifying the capacity in which they require admission and giving such other particulars as the Director may reasonably require;

14.1.2 ensure that all Supplier Personnel:

(a) are appropriately qualified, trained and experienced to provide the Services with all reasonable skill, care and diligence;

(b) are vetted in accordance with Good Industry Practice and, where applicable, the security requirements set out in Schedule 2.1 (*Services Description*) and Schedule 2.4 (*Security Management*); and

(c) comply with all reasonable requirements of the Director concerning conduct at the Director Premises, including the security requirements as set out in Schedule 2.4 (*Security Management*);

14.1.3 subject to Schedule 9.1 (*Staff Transfer*), retain overall control of the Supplier Personnel at all times so that the Supplier Personnel shall not be deemed to be employees, agents or contractors of the Director;

14.1.4 be liable at all times for all acts or omissions of Supplier Personnel, so that any act or omission of a member of any Supplier Personnel which results in a Default under this Agreement shall be a Default by the Supplier;

14.1.5 use all reasonable endeavours to minimise the number of changes in Supplier Personnel;

14.1.6 replace (temporarily or permanently, as appropriate) any Supplier Personnel as soon as practicable if any Supplier Personnel have been removed or are unavailable for any reason whatsoever;

14.1.7 bear the programme familiarisation and other costs associated with any replacement of any Supplier Personnel; and

14.1.8 procure that the Supplier Personnel shall vacate the Director Premises immediately upon the termination or expiry of this Agreement.

14.2 If the Director reasonably believes that any of the Supplier Personnel are unsuitable to undertake work in respect of this Agreement, it may:

14.2.1 refuse admission to the relevant person(s) to the Director Premises; and/or

14.2.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s).

Key Personnel

14.3 The Supplier shall ensure that the Key Personnel fulfil the Key Roles at all times during the Term. Schedule 9.2 (*Key Personnel*) lists the Key Roles and names of the persons who the Supplier shall appoint to fill those Key Roles at the Effective Date.

14.4 The Director may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Personnel.

14.5 The Supplier shall not appoint, remove or replace any Key Personnel (including when carrying out Exit Management) unless:

14.5.1 requested to do so by the Director;

14.5.2 the person concerned resigns, retires or dies or is on maternity leave, paternity leave or shared parental leave or long-term sick leave;

14.5.3 the person's employment or contractual arrangement with the Supplier or a Sub-contractor is terminated for material breach of contract by the employee; or

14.5.4 the Supplier obtains the Director's prior written consent (such consent not to be unreasonably withheld or delayed).

14.6 The Supplier shall:

14.6.1 notify the Director promptly of the absence of any Key Personnel (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

14.6.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

14.6.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Personnel and, except in the cases of death, unexpected ill health or a material breach of the Key Personnel's employment contract, this will mean at least sixty (60) Working Days' notice. The Director shall have the right to review (including interviewing a prospective replacement), reject or request the replacement of any member of Key Personnel;

14.6.4 ensure that all arrangements for planned changes in Key Personnel provide adequate periods during which incoming and outgoing Key Personnel work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services; and

14.6.5 ensure that any replacement for a Key Role:

(a) has a level of qualifications and experience appropriate to the relevant Key Role; and

(b) is fully competent to carry out the tasks assigned to the Key Personnel whom he or she has replaced.

Employment Indemnity

14.7 The Parties agree that:

14.7.1 the Supplier shall both during and after the Term indemnify the Director against all Employee Liabilities that may arise as a result of any claims brought against the Director

by any person where such claim arises from any act or omission of the Supplier or any Supplier Personnel; and

14.7.2 the Director shall both during and after the Term indemnify the Supplier against all Employee Liabilities that may arise as a result of any claims brought against the Supplier by any person where such claim arises from any act or omission of the Director or any of the Director's employees, agents, consultants and contractors.

Income Tax and National Insurance Contributions

14.8 Where the Supplier or any Supplier Personnel are liable to be taxed in the UK or to pay national insurance contributions in respect of consideration received under this Agreement, the Supplier shall:

14.8.1 at all times comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, and the Social Security Contributions and Benefits Act 1992 and all other statutes and regulations relating to national insurance contributions, in respect of that consideration; and

14.8.2 indemnify the Director against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Supplier Personnel.

Staff Transfer

14.9 The Parties agree that:

14.9.1 where the commencement of the provision of the Services or any part of the Services results in one or more Relevant Transfers, Schedule 9.1 (*Staff Transfer*) shall apply as follows:

(a) where the Relevant Transfer involves the transfer of Transferring Former Supplier Employees, Part 2 and Part 4 of Schedule 9.1 (*Staff Transfer*) shall apply; and

(b) Part 1 and Part 3 of Schedule 9.1 (*Staff Transfer*) shall not apply;

14.9.2 where commencement of the provision of the Services or a part of the Services does not result in a Relevant Transfer, Part 3 of Schedule 9.1 (*Staff Transfer*) shall apply, Part 4 of Schedule 9.1 may apply and Parts 1 and 2 of Schedule 9.1 (*Staff Transfer*) shall not apply; and

14.9.3 Part 5 of Schedule 9.1 (*Staff Transfer*) shall apply on the expiry or termination of the Services or any part of the Services.

Real Living Wage

14.10 Unless otherwise agreed with the Director, from the Effective Date and throughout the Term, the Supplier shall:

14.10.1 pay all Supplier employees based in the UK the current Real Living Wage (or a local or regionally-recognised equivalent scheme) as a minimum rate;

14.10.2 encourage and promote to its Sub-contractors a commitment to the Real Living Wage and associated principles; and

14.10.3 promptly provide all such information as may be requested by the Director from time to time regarding the Supplier's compliance with this Clause 14.10.

14.11 If it is agreed with the Director under Clause 14.10 that the Supplier is not a Real Living Wage employer at the Effective Date, the Supplier shall commit to a timescale and plan for introducing the Real Living Wage across its organisation and also to commit to promoting a similar commitment through its Sub-contractors. Such plan must be agreed by the Director and reviewed at regular intervals. Failure to implement the agreed plan shall constitute a Notifiable Default under Clause 29.1.3.

Social Value

14.12 The Supplier shall comply with its obligations in respect of the social value plan set out in Schedule 4.1 (*Supplier Solution*).

15 SUPPLY CHAIN RIGHTS AND PROTECTIONS

Advertising Sub-contract Opportunities

15.1 The Supplier shall:

15.1.1 subject to Clauses 15.3 and 15.4, advertise on Contracts Finder all Sub-contract opportunities arising from the provision of the Services above a minimum threshold of £25,000 (twenty-five thousand pounds) that arise during the Term;

15.1.2 within ninety (90) days of awarding a Sub-contract to a Sub-contractor, update the notice on Contracts Finder with details of the successful Sub-contractor;

15.1.3 monitor the number, type and value of the Sub-contract opportunities placed on Contracts Finder, advertised and awarded in its supply chain during the Term;

15.1.4 provide reports on the information at Clause 15.1.3 to the Director in the format and frequency as reasonably specified by the Director; and

15.1.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

15.2 Each advert referred to in Clause 15.1 above shall provide a full and detailed description of the Sub-contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

15.3 The obligation at Clause 15.1 shall only apply in respect of Sub-contract opportunities arising after the Effective Date.

15.4 Notwithstanding Clause 15.1 the Director may, by giving its prior written approval, agree that a Sub-contract opportunity is not required to be advertised on Contracts Finder.

Appointment of Sub-contractors

15.5 The Supplier shall exercise due skill and care in the selection and appointment of any Sub-contractors to ensure that the Supplier is able to:

15.5.1 manage any Sub-contractors in accordance with Good Industry Practice;

15.5.2 comply with its obligations under this Agreement in the delivery of the Services; and

15.5.3 assign, novate or otherwise transfer to the Director or any Replacement Supplier any of its rights and/or obligations under each Sub-contract that relates exclusively to this Agreement.

15.6 Prior to sub-contracting any of its obligations under this Agreement, the Supplier shall notify the Director in writing of:

15.6.1 the proposed Sub-contractor's name, registered office and company registration number;

15.6.2 the scope of any Services to be provided by the proposed Sub-contractor; and

15.6.3 where the proposed Sub-contractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the Director that the proposed Sub-contract has been agreed on "arm's-length" terms.

15.7 If requested by the Director within ten (10) Working Days of receipt of the Supplier's notice issued pursuant to Clause 15.6, the Supplier shall also provide:

15.7.1 a copy of the proposed Sub-contract; and

15.7.2 any further information reasonably requested by the Director.

15.8 The Director may, within ten (10) Working Days of receipt of the Supplier's notice issued pursuant to Clause 15.6 (or, if later, receipt of any further information requested pursuant to Clause 15.7), object to the appointment of the relevant Sub-contractor if it considers that:

15.8.1 the appointment of a proposed Sub-contractor may prejudice the provision of the Services and/or may be contrary to the interests of the Director;

15.8.2 the proposed Sub-contractor is unreliable and/or has not provided reasonable services to its other customers;

15.8.3 the proposed Sub-contractor employs unfit persons; and/or

15.8.4 the proposed Sub-contractor should be excluded in accordance with Clause 15.18 (*Termination of Sub-contracts*);

in which case, the Supplier shall not proceed with the proposed appointment.

15.9 If:

15.9.1 the Director has not notified the Supplier that it objects to the proposed Sub-contractor's appointment by the later of ten (10) Working Days of receipt of:

(a) the Supplier's notice issued pursuant to Clause 15.6; and

(b) any further information requested by the Director pursuant to Clause 15.7; and

15.9.2 the proposed Sub-contract is not a Key Sub-contract (which shall require the written consent of the Director in accordance with Clause 15.10 (*Appointment of Key Sub-contractors*),

the Supplier may proceed with the proposed appointment and, where the Sub-contract is entered into exclusively for the purpose of delivery of the Services, shall notify the Director that the relevant Sub-contract shall constitute a Third Party Contract for the purposes of Schedule 4.4 (*Third Party Contracts*).

Appointment of Key Sub-contractors

15.10 Where the Supplier wishes to enter into a Key Sub-contract or replace a Key Sub-contractor, it must obtain the prior written consent of the Director, such consent not to be unreasonably withheld or delayed. For these purposes, the Director may withhold its consent to the appointment of a Key Sub-contractor if it reasonably considers that:

15.10.1 the appointment of a proposed Key Sub-contractor may prejudice the provision of the Services or may be contrary to the interests of the Director;

15.10.2 the proposed Key Sub-contractor is unreliable and/or has not provided reasonable services to its other customers; and/or

15.10.3 the proposed Key Sub-contractor employs unfit persons; and/or

15.10.4 the proposed Key Sub-contractor should be excluded in accordance with Clause 15.18 (*Termination of Sub-contracts*).

15.11 The Director consents to the appointment of the Key Sub-contractors listed in Schedule 4.3 (*Notified Key Sub-contractors*).

15.12 Except where the Director has given its prior written consent, the Supplier shall ensure that each Key Sub-contract shall include:

15.12.1 provisions which will enable the Supplier to discharge its obligations under this Agreement;

15.12.2 a right under CRTPA for the Director to enforce any provisions under the Key Sub-contract which are capable of conferring a benefit upon the Director;

15.12.3 a provision enabling the Director to enforce the Key Sub-contract as if it were the Supplier;

15.12.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-contract to the Director or any Replacement Supplier without restriction (including any need to obtain any consent or approval) or payment by the Director;

15.12.5 obligations no less onerous on the Key Sub-contractor than those imposed on the Supplier under this Agreement in respect of:

(a) data protection requirements set out in Clauses 22 (*Director Data and Security Requirements*) and 25 (*Protection of Personal Data*);

(b) FOIA requirements set out in Clause 24 (*Transparency and Freedom of Information*);

(c) the obligation not to embarrass the Director or otherwise bring the Director into disrepute set out in Clause 5.6.14 (*Services*);

(d) the keeping of records in respect of the services being provided under the Key Sub-contract, including the maintenance of Open Book Data; and

(e) the conduct of Audits set out in Part 3 of Schedule 7.5 (*Financial Reports, Audit, Risk and Compliance*);

15.12.6 provisions enabling the Supplier to terminate the Key Sub-contract on notice on terms no more onerous on the Supplier than those imposed on the Director under Clauses 35.1.1 (*Termination by the Director*) and 36.4 (*Payments by the Director*) and Schedule 7.2 (*Payments on Termination*) of this Agreement;

15.12.7 a provision restricting the ability of the Key Sub-contractor to sub-contract all or any part of the services provided to the Supplier under the Key Sub-contract without first seeking the written consent of the Director;

15.12.8 a provision enabling the Supplier or the Director to appoint a Remedial Adviser on substantially the same terms as are set out in Clause 31 (*Remedial Adviser*);

15.12.9 a provision enabling the Supplier, the Director or any other person on behalf of the Director to step-in on substantially the same terms as are set out in Clause 32 (*Step-in Rights*);

15.12.10 a provision requiring the Key Sub-contractor to participate in, and if required by the Director in the relevant Multi-Party Procedure Initiation Notice to procure the participation of all or any of its Sub-contractors in, the Multi-Party Dispute Resolution Procedure; and

15.12.11 a provision requiring the Key Sub-contractor to:

(a) promptly notify the Supplier and the Director in writing of any of the following of which it is, or ought to be, aware:

(i) the occurrence of a Financial Distress Event in relation to the Key Sub-contractor; or

(ii) any fact, circumstance or matter of which it is aware which could cause the occurrence of a Financial Distress Event in relation to the Key Sub-contractor,

and in any event, provide such notification within ten (10) Working Days of the date on which the Key Sub-contractor first becomes aware of such; and

(b) co-operate with the Supplier and the Director in order to give full effect to the provisions of Schedule 7.4 (*Financial Distress*), including meeting with the Supplier and the Director to discuss and review the effect of the Financial Distress Event on the continued performance and delivery of the Services, and contributing to and complying with the Financial Distress Remediation Plan, and providing the information specified at paragraph 4.3.2(b) of Schedule 7.4 (*Financial Distress*).

15.12.12 a provision requiring the Key Sub-contractor to enter into a direct confidentiality agreement with the Director on the same terms as set out in Clause 23 (*Confidentiality*);

15.12.13 a provision requiring the Key Sub-contractor to comply with the obligations set out in Clause 37.3 (*Equality and Diversity*);

15.12.14 a provision requiring the Key Sub-contractor to comply with the obligations substantially the same as those set out in Clause 42 (*Conflicts of Interest*);

15.12.15 a provision requiring the Key Sub-contractor to have in place an appropriate exit and migration plan which enables it to comply (and will enable to the Supplier to comply) with the requirements of this Agreement, to put such plan into effect on any termination or expiry of the Sub-contract and otherwise to ensure that any such termination or expiry will not affect the continuity of Services;

15.12.16 a provision requiring the Key Sub-contractor to notify the Director promptly in writing of any material non-payment or late payment of any sums properly due to the Key Sub-contractor from the Supplier under a valid invoice under the Key Sub-contract and not subject to a genuine dispute; and

15.12.17 the following wording (amended only as appropriate to conform with the layout of and definitions in the Key Sub-contract):

"The Key Sub-contractor shall not exercise any right to terminate the Key Sub-contract without having first given the Director at least six (6) months' advance notice in writing. In any situation where either (1) the Key Sub-contractor has the right to terminate the Key Sub-contract otherwise than for convenience or (2) the Director has the right to terminate this Agreement other than by reason of convenience or step into this Agreement pursuant to Clause 32 (*Step-In Rights*), then the Director may require that the rights and obligations of the Supplier under the Key Sub-contract to be assigned or novated to the Director either permanently or for such a period as the Director may specify and the Key Sub-contractor shall consent to such assignment or novation and continue to perform the Key Sub-Contract directly for the benefit of the Director."

15.13 In the event that the Director has a right to terminate this Agreement otherwise than for convenience or to step-in to the performance of the Services pursuant to Clause 32 (*Step-in Rights*), the Director may enter into an agreement with the Key Sub-contractor which has the effect of assigning or novating any or all of the Supplier's rights and obligations under the relevant Key Sub-contract pursuant to Clause 15.12.4 without the Supplier's prior written consent and the Supplier shall enter into such agreement and/or deed in accordance with Clause 44 (*Further Assurances*) as the Director reasonably requires so as to give effect to such assignment or novation. If the Director does require an assignment or novation pursuant to this Clause 15.13, the Supplier shall automatically be relieved to that extent of its obligations to provide Services under this Agreement and the Director's obligations to pay the Charges shall be reduced proportionately.

15.14 The Supplier shall not terminate or materially amend the terms of any Key Sub-contract without the Director's prior written consent, which shall not be unreasonably withheld or delayed.

Supply chain protection

15.15 The Supplier shall ensure that all Sub-contracts (which in this Clause 15.15 includes any contract in the Supplier's supply chain made wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Agreement) contain provisions:

15.15.1 giving the Supplier a right to terminate the Sub-contract if the Sub-contractor fails to comply in the performance of the Sub-contract with legal obligations in the fields of environmental, social or labour law;

15.15.2 requiring the Supplier or other party receiving goods or services under the contract to consider and verify invoices under that contract in a timely fashion;

15.15.3 that if the Supplier or other party fails to consider and verify an invoice in accordance with Clause 15.15.2, the invoice shall be regarded as valid and undisputed for the purpose of Clause 15.15.4 after a reasonable time has passed;

15.15.4 requiring the Supplier or other party to pay any undisputed sums which are due from it to the Sub-contractor within a specified period not exceeding thirty (30) days of verifying that the invoice is valid and undisputed;

15.15.5 giving the Director a right to publish the Supplier's compliance with its obligation to pay undisputed invoices within the specified payment period; and

15.15.6 requiring the Sub-contractor to include a clause to the same effect as this Clause 15.15 in any contracts it enters into wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Agreement.

15.16 The Supplier shall pay any undisputed sums which are due from it to a Sub-contractor within thirty (30) days of verifying that the invoice is valid and undisputed.

15.17 Notwithstanding any provision of Clauses 23 (*Confidentiality*) and 26 (*Publicity and Branding*), if the Supplier notifies the Director that the Supplier has failed to pay a Sub-contractor's undisputed invoice within thirty (30) days of receipt or that it has failed to pay 95% or above of its Sub-contractors or Unconnected Sub-contractors within sixty (60) days after the day on which the Supplier receives an invoice or otherwise has notice of an amount for payment, or the Director otherwise discovers the same, the Director shall be entitled to publish the details of the late or non-payment (including on government websites and in the press).

Termination of Sub-contracts

15.18 The Director may require the Supplier to terminate:

15.18.1 a Sub-contract where:

(a) the acts or omissions of the relevant Sub-contractor have caused or materially contributed to the Director's right of termination pursuant to Clause 35.1.2 (*Termination by the Director*);

(b) the relevant Sub-contractor or any of its Affiliates have embarrassed the Director or otherwise brought the Director into disrepute by engaging in any act or omission which is reasonably likely to diminish the trust that the public places in the Director, regardless of whether or not such act or omission is related to the Sub-contractor's obligations in relation to the Services or otherwise;

(c) the relevant Sub-contractor has failed to comply in the performance of its Sub-contract with legal obligations in the fields of environmental, social or labour law; and/or

(d) the Director has found grounds for exclusion of the Sub-contractor in accordance with Clause 15.23; and

15.18.2 a Key Sub-contract where there is a change of Control of the relevant Key Sub-contractor, unless:

(a) the Director has given its prior written consent to the particular change of Control, which subsequently takes place as proposed; or

(b) the Director has not served its notice of objection within six (6) months of the later of the date the change of Control took place or the date on which the Director was given notice of the change of Control.

Competitive Terms

15.19 If the Director is able to obtain from any Sub-contractor or any other third party (on a like-for-like basis) more favourable commercial terms with respect to the supply of any goods, software or services used by the Supplier or the Supplier Personnel in the supply of the Services, then the Director may require the Supplier to replace its existing commercial terms with that person with the more favourable commercial terms obtained by the Director in respect of the relevant item.

15.20 If the Director exercises its option pursuant to Clause 15.19, then the Charges shall be reduced by an amount that is agreed in accordance with the Change Control Procedure.

15.21 Not used

Retention of Legal Obligations

15.22 Notwithstanding the Supplier's right to sub-contract pursuant to this Clause 15, the Supplier shall remain responsible for all acts and omissions of its Sub-contractors and the acts and omissions of those employed or engaged by the Sub-contractors as if they were its own. In respect of any element of the Services delivered by Supplier Personnel and/or which are Sub-contracted by the Supplier, an obligation on the Supplier to do or to refrain from doing any act or thing under this Agreement, shall include an obligation on the Supplier to procure that the Supplier Personnel and the Sub-contractor also do or refrain from doing such act or thing in their delivery of those elements of the Services.

Exclusion of Sub-contractors

15.23 Where the Director considers whether there are grounds for the exclusion of a Sub-contractor under Regulation 57 of the Public Contracts Regulations 2015, then:

15.23.1 if the Director finds there are compulsory grounds for exclusion, the Supplier shall replace or shall not appoint the Sub-contractor; or

15.23.2 if the Director finds there are non-compulsory grounds for exclusion, the Director may require the Supplier to replace or not to appoint the Sub-contractor and the Supplier shall comply with such a requirement.

Reporting SME/VCSE Sub-contracts

15.24 In addition to any other Management Information requirements set out in this Agreement, the Supplier agrees that it shall, at no charge, provide timely, full, accurate and complete Supply Chain Transparency Information Reports to the Director thirty (30) days prior to the of the end of each financial year by providing all of the information described in the Supply Chain Transparency Information Template in the format set out in Schedule 8.4 (*Reports and Records Provisions*) Annex 4 and in accordance with any guidance issued by the Director from time to time.

15.25 The Director may update the Supply Chain Transparency Information Template from time to time (including the data required and/or format) by issuing a replacement version with at least thirty (30) days' notice and specifying the date from which it must be used.

SECTION F – INTELLECTUAL PROPERTY, DATA AND CONFIDENTIALITY

16 INTELLECTUAL PROPERTY RIGHTS

16.1 Except as expressly set out in this Agreement:

16.1.1 the Director shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Supplier or its licensors, namely:

(a) the Supplier Software;

(b) the Third Party Software

(c) the Third Party IPR's; and

(d) the Supplier Background IPRs;

16.1.2 the Supplier shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Director or its licensors, including:

(a) the Director Software;

(b) the Director Data; and

(c) the Director Background IPRs; and

16.1.3 Specially Written Software and Project Specific IPRs (except for any Know-How, trade secrets or Confidential Information contained therein) shall be the property of the Director.

16.2 Where either Party acquires, by operation of law, title to Intellectual Property Rights that is inconsistent with the allocation of title set out in Clause 16.1, it shall assign in writing such Intellectual Property Rights as it has acquired to the other Party on the request of the other Party (whenever made).

16.3 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

16.4 Unless the Director otherwise agrees in advance in writing:

16.4.1 all Specially Written Software and any software element of Project Specific IPRs shall be created in a format, or able to be converted into a format, which is suitable for publication by the Director as Open Source software; and

16.4.2 where the Specially Written Software and any software element of Project Specific IPRs are written in a format that requires conversion before publication as Open Source software, the Supplier shall also provide the converted format to the Director.

16.5 Where the Director agrees that any Specially Written Software and/or any software element of Project Specific IPRs should be excluded from Open Source publication, the Supplier shall as soon as reasonably practicable provide written details of the impact that such exclusion will have on the Director's ability to publish other Open Source software under Clause 21 (*Open Source Publication*).

17 TRANSFER AND LICENCES GRANTED BY THE SUPPLIER

Specially Written Software and Project Specific IPRs

17.1 The Supplier hereby agrees to transfer to the Director, or shall procure the transfer to the Director of:

17.1.1 all rights (subject to Clause 16.1.1 (*Intellectual Property Rights*)) in the Specially Written Software and the Project Specific IPRs including (without limitation);

(a) the Documentation, Source Code and the Object Code of the Specially Written Software; and

(b) all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software (together the "**Software Supporting Materials**");

but not including any Know-How, trade secrets or Confidential Information.

17.2 The Supplier:

17.2.1 shall:

(a) inform the Director of all Specially Written Software and any element of Project Specific IPRs that constitutes a modification or enhancement to Supplier Software or Third Party Software; and

(b) deliver to the Director the Specially Written Software and the software element of Project Specific IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven (7) days of the issue of a Milestone Achievement Certificate in respect of the relevant Deliverable and shall provide updates of the Source Code and of the Software Supporting Materials promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Director; and

(c) without prejudice to Clause 17.9 (*Third Party Software and Third Party IPRs*), provide full details to the Director of any Supplier Background IPRs or Third Party IPRs which are embedded in or which are an integral part of the Specially Written Software or any element of Project Specific IPRs;

17.2.2 acknowledges and agrees that the ownership of the media referred to in Clause 17.2.1(b) shall vest in the Director upon their receipt by the Director; and

17.2.3 shall execute all such assignments as are required to ensure that any rights in the Specially Written Software and Project Specific IPRs are properly transferred to the Director.

Supplier Software and Supplier Background IPRs

17.3 The Supplier shall not use any Supplier Non-COTS Software or Supplier Non-COTS Background IPR in the provision of the Services unless it is detailed in Schedule 5.1 (*Software*) or sent to the relevant governance body for review and approval granted by the Director.

17.4 The Supplier hereby grants to the Director:

17.4.1 a perpetual, royalty-free and non-exclusive licence to use (including but not limited to the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display)) the Supplier Non-COTS Software and Supplier Non-COTS Background IPR for which the Supplier delivers a copy to the Director for any purpose relating to the Services (or substantially equivalent services) or for any purpose relating to the exercise of the Director's (or any other Central Government Body's) business or function;

17.4.2 a perpetual, royalty free and non-exclusive licence to use the Supplier COTS Software for which the Supplier delivers a copy to the Director and Supplier COTS Background IPRs on the licence terms identified in a letter in or substantially in the form set out in Annex 1 to Schedule 5.1 (*Software*) and signed by or on behalf of the Parties on or before the Effective Date, provided always that, notwithstanding the terms incorporated in Schedule 5.1 (*Software*) the licence shall be granted on a perpetual basis and the Director shall remain entitled to sub-license and to assign and novate the Supplier COTS Software and Supplier COTS Background IPRs on equivalent terms to those set out in Clauses 17.5 (*Director's right to sub-licence*) and 17.6 (*Director's right to assign/novate sub-licences*) in relation to the Supplier Non-COTS Software and Supplier Non-COTS Background IPRs; and

17.4.3 a perpetual royalty-free non-exclusive licence to use without limitation any Know-How, trade secrets or Confidential Information contained within the Specially Written Software or the Project Specific IPRs.

Director's right to sub-license

17.5 The Director may sub-license:

17.5.1 the rights granted under Clause 17.4.1 (*Supplier Software and Supplier Background IPRs*) to a third party (including for the avoidance of doubt, to any Replacement Supplier or Relevant Third Party Supplier) provided that:

(a) the sub-licence is on terms no broader than those granted to the Director;

(b) the sub-licence authorises the third party to use the rights licensed in Clause 17.4.1 (*Supplier Software and Supplier Background IPRs*) only for purposes relating to the Services (or substantially equivalent services), the Related Services or for any purpose relating to the exercise of the Director's (or any other Central Government Body's) business or function; and

(c) the sub-licensee shall have executed a confidentiality undertaking in favour of the Supplier in or substantially in the form set out in Annex 2 to Schedule 5.1 (*Software*); and

17.5.2 the rights granted under Clause 17.4.1 (*Supplier Software and Supplier Background IPRs*) to any Approved Sub-Licensee to the extent necessary to use and/or obtain the benefit of the Project Specific IPRs provided that:

(a) the sub-licence is on terms no broader than those granted to the Director; and

(b) the Supplier has received a confidentiality undertaking in its favour in or substantially in the form set out in Annex 2 to Schedule 5.1 (*Software*) duly executed by the Approved Sub-Licensee.

Director's right to assign/novate licences

17.6 The Director may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Clause 17.4.1 (*Supplier Software and Supplier Background IPRs*) to:

17.6.1 a Central Government Body; or

17.6.2 to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Director.

17.7 Any change in the legal status of the Director which means that it ceases to be a Central Government Body shall not affect the validity of any licence granted in Clause 17.4 (*Supplier Software and Supplier Background IPRs*). If the Director ceases to be a Central Government Body, the successor body to the Director shall still be entitled to the benefit of the licence granted in Clause 17.4 (*Supplier Software and Supplier Background IPRs*).

17.8 If a licence granted in Clause 17.4 (*Supplier Software and Supplier Background IPRs*) is novated under Clause 17.6 (*Director's right to assign/novate licences*) or there is a change of the Director's status pursuant to Clause 17.7, the rights acquired on that novation or change of status shall not extend beyond those previously enjoyed by the Director.

Third Party Software and Third Party IPRs

17.9 The Supplier shall not use in the provision of the Services (including in any Specially Written Software or in the software element of Project Specific IPRs) any Third Party Non-COTS Software or Third Party Non-COTS IPRs unless detailed in Schedule 5.1 (*Software*) or approval is granted by the Director following a review by the relevant governance body and has in each case either:

17.9.1 first procured that the owner or an authorised licensor of the relevant Third Party Non-COTS IPRs or Third Party Non-COTS Software (as the case may be) has granted a direct licence to the Director on a perpetual, royalty-free basis to the Director and on terms no less favourable to the Director than those set out in Clauses 17.4.1 (*Supplier Software and Supplier Background IPRs*) and 17.5 (*Director's right to sub-licence*) and Clause 17.6 (*Director's right to assign/novate licences*); or

17.9.2 complied with the provisions of Clause 17.10.

17.10 If the Supplier cannot obtain for the Director a licence in respect of any Third Party Non-COTS Software and/or Third Party Non-COTS IPRs in accordance with the licence terms set out in Clause 17.9.1, the Supplier shall:

17.10.1 notify the Director in writing giving details of what licence terms can be obtained from the relevant third party and whether there are alternative software providers which the Supplier could seek to use; and

17.10.2 use the relevant Third Party Non-COTS Software and/or Third Party Non-COTS IPRs only if the Director has first approved in writing the terms of the licence from the relevant third party.

17.11 The Supplier shall:

17.11.1 notify the Director in writing of all Third Party COTS Software and Third Party COTS IPRs that it uses and the terms on which it uses them; and

17.11.2 unless instructed otherwise in writing by the Director in any case within twenty (20) Working Days of notification pursuant to Clause 17.10.1, use all reasonable endeavours to procure in each case that the owner or an authorised licensor of the relevant Third Party COTS Software and Third Party COTS IPRs grants a direct licence to the Director on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the relevant third party.

17.12 Should the Supplier become aware at any time, including after termination, that the Specially Written Software and/or the Project Specific IPRs contain any Intellectual Property Rights for which the Director does not have a suitable licence, then the Supplier must notify the Director within ten (10)

days of what those rights are and which parts of the Specially Written Software and the Project Specific IPRs they are found in.

Termination and Replacement Suppliers

17.13 For the avoidance of doubt, the termination or expiry of this Agreement shall not of itself result in any termination of any of the licences granted by the Supplier or relevant third party pursuant to or as contemplated by this Clause 17.

17.14 The Supplier shall, if requested by the Director in accordance with Schedule 8.5 (*Exit Management*) and at the Supplier's cost:

17.14.1 grant (or procure the grant) to any Replacement Supplier of:

(a) a licence to use any Supplier Non-COTS Software, Supplier Non-COTS Background IPRs, Third Party Non-COTS IPRs and/or Third Party Non-COTS Software on a royalty-free basis to the Replacement Supplier and on terms no less favourable than those granted to the Director in respect of the relevant Software and/or IPRs pursuant to or as contemplated by this Clause 17 subject to receipt by the Supplier of a confidentiality undertaking in its favour in or substantially in the form set out in Annex 2 to Schedule 5.1 (*Software*) duly executed by the Replacement Supplier;

(b) a licence to use any Supplier COTS Software and/or Supplier COTS Background IPRs, on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the Supplier; and/or

17.14.2 use all reasonable endeavours to procure the grant to any Replacement Supplier of a licence to use any Third Party COTS Software and/or Third Party COTS IPRs on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the relevant third party; and/or

17.14.3 assign or novate any licences granted by the Supplier or relevant third party to the Director and/or the Replacement Supplier.

18 ESCROW

18.1 The Supplier shall deposit the Source Code, of such part of the Software that the Director, acting reasonably requires the Supplier to place in escrow, with the NCC on the standard NCC Software Escrow Terms not less than ten (10) Working Days of the Director's request. The Supplier shall ensure that the deposited version of the Source Code is the current version of the Deposited Software and that the deposited version is kept up-to-date as the Deposited Software is modified or upgraded. The Supplier shall pay the initial deposit and storage fees under the escrow agreement and the Director shall be responsible for paying the release fees.

18.2 Where the Supplier is unable to procure compliance with the provisions of Clause 18 in respect of any Third Party Software, it shall provide the Director with written evidence of its inability to comply with these provisions and shall agree with the Director a suitable alternative to escrow that affords the Director the nearest equivalent protection. The Supplier shall be excused from its obligations under Clause 18 only to the extent that the Parties have agreed on a suitable alternative.

18.3 In circumstances where the Director obtains the release of the Source Code from escrow, the Supplier hereby grants (or shall procure the grant) to the Director a perpetual, royalty-free and non-exclusive licence, with a right to sub-license, to use and support the Source Code version of the Deposited Software to the extent necessary for the receipt of the Services or any Replacement Services.

19 LICENCES GRANTED BY THE DIRECTOR

19.1 The Director hereby grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Term to use the Director Software, the Director Background IPRs, the Specially Written

Software, the Project Specific IPRs and the Director Data solely to the extent necessary for performing the Services in accordance with this Agreement, including (but not limited to) the right to grant sub-licences to Sub-contractors provided that:

19.1.1 any relevant Sub-contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 23 (*Confidentiality*); and

19.1.2 the Supplier shall not, without the Director's prior written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Director.

19.2 The Director hereby grants to the Supplier (and to any Key Sub-contractors approved in accordance with Clause 15.10) a royalty-free, non-exclusive, non-transferable licence in the Territory during the Term to use the Trade Marks in relation to the provision of the Services from the Effective Date and subject to the terms of use set out in Schedule 5.2 (*Trade Mark Licence Terms*).

19.3 The Director may terminate any licence to the Trade Marks (or part thereof) and require the Supplier to cease use of or replace any of the Trade Marks at any time for any reason by immediate written notice.

19.4 For the avoidance of doubt, the Director may also terminate any licence to the Trade Marks (or part thereof) by immediate written notice in the event that the Supplier:

19.4.1 commits a breach of the terms of the Trade Mark Licence;

19.4.2 challenges the validity of the Trade Marks or any of them; and/or

19.4.3 tries to take any steps to allow others to try to register, use or cancel any of the Trade Marks or any trade mark similar to any of them.

19.5 If the Director exercises its rights to terminate the Trade Mark Licence (in whole or in part) pursuant to either Clause 19.3 or Clause 19.4 the Supplier shall:

19.5.1 immediately cease all use of the Trade Marks (or the relevant Trade Marks as the case may be);

19.5.2 promptly make any necessary updates in respect of the use of the relevant Trade Marks or replacement Trade Marks for all Customer-facing materials;

19.5.3 at the discretion of the Director, return or destroy documents and other tangible materials that contain any of the Trade Marks, provided that if the Director has not made an election within six (6) months of the termination, the Supplier may destroy the documents and other tangible materials that contain any of the Trade Marks (as the case may be); and

19.5.4 ensure, so far as reasonably practicable, that any copies of the Trade Marks that are held in electronic, digital or other machine readable form ceases to be readily accessible from any Supplier computer, word processor, voicemail system or any other Supplier device containing copies of such Trade Marks.

19.6 If the Director exercises its rights to terminate the Trade Mark Licence as a whole or does not confirm a revised or a replacement Trade Mark for use in the case of a partial termination, the parties shall meet and discuss in good faith the implications such termination will have on the provision of the Services.

19.7 In the event of the termination or expiry of this Agreement, the licences granted pursuant to this Clause 19, including any Trade Mark Licence and any sub-licence granted by the Supplier in accordance with Clause 19.1 shall terminate automatically on the date of such termination or expiry and the Supplier shall:

19.7.1 immediately cease all use of the Trade Marks, Director Software, the Director Background IPRs and the Director Data (as the case may be);

19.7.2 at the discretion of the Director, return or destroy documents and other tangible materials that contain any of the Director Software, the Director Background IPRs and the Director Data, provided that if the Director has not made an election within six (6) months of the termination of the licence, the Supplier may destroy the documents and other tangible materials that contain any of the Director Software, the Director Background IPRs and the Director Data (as the case may be); and

19.7.3 ensure, so far as reasonably practicable, that any Director Software, Director Background IPRs and Director Data that are held in electronic, digital or other machine readable form ceases to be readily accessible from any Supplier computer, word processor, voicemail system or any other Supplier device containing such Director Software, Director Background IPRs and/or Director Data.

20 IPRS INDEMNITY

20.1 The Supplier shall at all times, during and after the Term, on written demand indemnify the Director and each other Indemnified Person, and keep the Director and each other Indemnified Person indemnified, against all Losses incurred by, awarded against or agreed to be paid by an Indemnified Person arising from an IPRs Claim.

20.2 If an IPRs Claim is made, or the Supplier anticipates that an IPRs Claim might be made, the Supplier may, at its own expense and sole option, either:

20.2.1 procure for the Director or other relevant Indemnified Person the right to continue using the relevant item which is subject to the IPRs Claim; or

20.2.2 replace or modify the relevant item with non-infringing substitutes provided that:

(a) the performance and functionality of the replaced or modified item is at least equivalent to the performance and functionality of the original item;

(b) the replaced or modified item does not have an adverse effect on any other Services or the IT Environment;

(c) there is no additional cost to the Director or relevant Indemnified Person (as the case may be); and

(d) the terms and conditions of this Agreement shall apply to the replaced or modified Services.

20.3 If the Supplier elects to procure a licence in accordance with Clause 20.2.1 or to modify or replace an item pursuant to Clause 20.2.2, but this has not avoided or resolved the IPRs Claim, then:

20.3.1 the Director may terminate this Agreement (if subsisting) with immediate effect by written notice to the Supplier; and

20.3.2 without prejudice to the indemnity set out in Clause 20.1, the Supplier shall be liable for all reasonable and unavoidable costs of the substitute items and/or services including the additional costs of procuring, implementing and maintaining the substitute items.

20.4 Subject to Clause 27.6.2, the Director agrees to indemnify and hold harmless the Supplier against all Losses arising directly out of any claim by a third party that the normal use or possession of an item for which the Director is responsible for delivering to the Supplier for the purposes of the provision of the Services during the performance of the Agreement ("**Item**") infringes the intellectual property rights of that third party subject to the following conditions:

20.4.1 the Supplier shall promptly notify the Director in writing of any allegations of infringement of which it has notice and will not make any admissions of liability or otherwise without the Director's prior written consent;

20.4.2 the Supplier, at the Director's request and expense, shall allow the Director to conduct and/or settle all negotiations and litigation resulting from any such claim taking into account the reasonable representations of the Supplier; and

20.4.3 the Supplier shall, at the request of the Director, afford all reasonable assistance with such negotiations or litigation and shall be reimbursed by the Director for any reasonable external expenses incurred in so doing.

This indemnity does not apply to the extent that a claim arises directly or indirectly from specifications, written information, or materials provided by the Supplier.

21 OPEN SOURCE PUBLICATION

21.1 The Supplier agrees that the Director may at its sole discretion publish as Open Source software all or part of the Specially Written Software and any software element of the Project Specific IPRs after the Operational Service Commencement Date.

21.2 The Supplier hereby warrants that the Specially Written Software and any software element of the Project Specific IPRs:

21.2.1 are suitable for release as Open Source and that any release will not allow a third party to use the Open Source software to in any way compromise the operation, running or security of the Specially Written Software, the Project Specific IPRs or the Director System;

21.2.2 shall not cause any harm or damage to any party using anything published as Open Source and that the Specially Written Software and the Project Specific IPRs do not contain any Malicious Software;

21.2.3 do not contain any material which would bring the Director into disrepute upon publication as Open Source;

21.2.4 do not contain any IPR owned or claimed to be owned by any third party which is found, or alleged to be found, in the Specially Written Software and the Project Specific IPRs ("**Non-Party IPRs**"); and

21.2.5 will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the Operational Service Commencement Date.

21.3 The Supplier shall ensure that the Open Source Publication Material provided to the Director does not include any Supplier Software or Supplier Background IPRs save that which the Supplier is willing to allow to be included in any Open Source publication. In such a case, the Supplier hereby acknowledges that any such Supplier Software or Supplier Background IPRs will become Open Source and will be licensed and treated as such following publication by the Director and any third party that uses the Open Source Publication Materials on the terms of the Open Source licence used by the Director when publishing as Open Source.

21.4 The Supplier hereby indemnifies the Director against all claims in which the Director is, or is threatened to be, a party for any alleged infringement of any Non-Party IPRs arising from publication of the Specially Written Software and any software element of the Project Specific IPRs as Open Source under Clause 21.1.

22 DIRECTOR DATA AND SECURITY REQUIREMENTS

22.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Director Data.

22.2 The Supplier shall not store, copy, disclose, or use the Director Data except as necessary for the performance by the Supplier of its obligations under this Agreement or as otherwise expressly authorised in writing by the Director.

22.3 To the extent that Director Data is held and/or processed by the Supplier, the Supplier shall supply that Director Data to the Director in such non-proprietary format as the Director may direct from time to time.

22.4 The Supplier shall preserve the integrity of Director Data and prevent the corruption or loss of Director Data at all times that the relevant Director Data is under its control or the control of any Sub-contractor.

22.5 The Supplier shall perform secure back-ups of all Director Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Service Continuity Plan. The Supplier shall ensure that such back-ups are available to the Director (or to such other person as the Director may direct) at all times upon request and are delivered to the Director at no less than six (6) monthly intervals (or such other intervals as may be agreed in writing between the Parties).

22.6 The Supplier shall ensure that any system on which the Supplier holds any Director Data, including back-up data, is a secure system that complies with the Baseline Security Requirements.

22.7 If the Director Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Director may:

22.7.1 require the Supplier (at the Supplier's expense) to restore or procure the restoration of Director Data to the extent and in accordance with the requirements specified in Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*) and the Supplier shall do so as soon as practicable but not later than five (5) Working Days from the date of receipt of the Director's notice; and/or

22.7.2 itself restore or procure the restoration of Director Data, and shall be repaid by the Supplier any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

22.8 If at any time the Supplier suspects or has reason to believe that Director Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Director immediately and inform the Director of the remedial action the Supplier proposes to take.

22.9 The Supplier shall at all times comply with the requirements of Schedule 2.4 (*Security Management*).

22.10 The Director shall notify the Supplier of any changes or proposed changes to the Baseline Security Requirements.

22.11 Subject to Clause 13.2 (*Change in Law*), if the Supplier believes that a change or proposed change to the Baseline Security Requirements will have a material and unavoidable cost implication to the Services it may submit a Change Request. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. If the Change is deemed to be a Specific Change in Law in accordance with Clause 13.2 (*Change in Law*), any change to the Charges shall then be agreed in accordance with the Change Control Procedure.

22.12 Until and/or unless a change to the Charges is agreed by the Director pursuant to Clause 22.11 the Supplier shall continue to perform the Services in accordance with its existing obligations.

23 CONFIDENTIALITY

23.1 For the purposes of this Clause 23, the term "**Disclosing Party**" shall mean a Party which discloses or makes available directly or indirectly its Confidential Information and "**Recipient**" shall mean the Party which receives or obtains directly or indirectly Confidential Information.

23.2 Except to the extent set out in this Clause 23 or where disclosure is expressly permitted elsewhere in this Agreement, the Recipient shall:

23.2.1 treat the Disclosing Party's Confidential Information as confidential and keep it in secure custody (which is appropriate depending upon the form in which such materials are stored and the nature of the Confidential Information contained in those materials);

23.2.2 not disclose the Disclosing Party's Confidential Information to any other person except as expressly set out in this Agreement or without obtaining the owner's prior written consent;

23.2.3 not use or exploit the Disclosing Party's Confidential Information in any way except for the purposes anticipated under this Agreement; and

23.2.4 immediately notify the Disclosing Party if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Disclosing Party's Confidential Information.

23.3 The Recipient shall be entitled to disclose the Confidential Information of the Disclosing Party where:

23.3.1 the Recipient is required to disclose the Confidential Information by Law, provided that Clause 24 (*Transparency and Freedom of Information*) shall apply to disclosures required under the FOIA or the EIRs;

23.3.2 the need for such disclosure arises out of or in connection with:

(a) any legal challenge or potential legal challenge against the Director arising out of or in connection with this Agreement;

(b) the examination and certification of the Director's accounts (provided that the disclosure is made on a confidential basis) or for any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Director is making use of any Services provided under this Agreement; or

(c) the conduct of a Central Government Body review in respect of this Agreement; or

23.3.3 the Recipient has reasonable grounds to believe that the Disclosing Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010 and the disclosure is being made to the Serious Fraud Office.

23.4 If the Recipient is required by Law to make a disclosure of Confidential Information, the Recipient shall as soon as reasonably practicable and to the extent permitted by Law notify the Disclosing Party of the full circumstances of the required disclosure including the relevant Law and/or regulatory body requiring such disclosure and the Confidential Information to which such disclosure would apply.

23.5 The Supplier may disclose the Confidential Information of the Director (or Confidential Information of a Relevant Third Party Supplier in accordance with the Collaboration Agreement) on a confidential basis only to:

23.5.1 Supplier Personnel who are directly involved in the provision of the Services and need to know the Confidential Information to enable performance of the Supplier's obligations under this Agreement;

23.5.2 its auditors; and

23.5.3 its professional advisers for the purposes of obtaining advice in relation to this Agreement.

Where the Supplier discloses Confidential Information of the Director pursuant to this Clause 23.5, it shall remain responsible at all times for compliance with the confidentiality obligations set out in this Agreement by the persons to whom disclosure has been made.

23.6 The Director may disclose the Confidential Information of the Supplier:

23.6.1 on a confidential basis to any Central Government Body for any proper purpose of the Director or of the relevant Central Government Body;

23.6.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

23.6.3 to the extent that the Director (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

23.6.4 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 23.6.1 (including any benchmarking organisation) for any purpose relating to or connected with this Agreement and/or to a Relevant Third Party Supplier pursuant to the Collaboration Agreement;

23.6.5 on a confidential basis for the purpose of the exercise of its rights under this Agreement, including the Audit Rights, its step-in rights pursuant to Clause 32 (*Step-In Rights*), its rights to appoint a Remedial Adviser pursuant to Clause 31 (*Remedial Adviser*) and Exit Management rights; or

23.6.6 on a confidential basis to a proposed Successor Body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Agreement,

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Director under this Clause 23.

23.7 Nothing in this Clause 23 shall prevent a Recipient from using any techniques, ideas or Know-How gained during the performance of this Agreement in the course of its normal business to the extent that this use does not result in a disclosure of the Disclosing Party's Confidential Information or an infringement of Intellectual Property Rights.

24 TRANSPARENCY AND FREEDOM OF INFORMATION

24.1 The Parties acknowledge that:

24.1.1 the Transparency Reports;

24.1.2 the content of this Agreement, including any changes to this Agreement agreed from time to time, except for:

(a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Director; and

(b) Commercially Sensitive Information; and

24.1.3 the Publishable Performance Information,

(together the "**Transparency Information**") are not Confidential Information.

24.2 Notwithstanding any other provision of this Agreement, the Supplier hereby gives its consent for the Director to publish to the general public the Transparency Information in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted). The Director shall, prior to publication, consult with the Supplier on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decision in its absolute discretion.

24.3 The Supplier shall assist and co-operate with the Director to enable the Director to publish the Transparency Information, including the preparation of the Transparency Reports in accordance with Paragraph 1 of Schedule 8.4 (*Reports and Records Provisions*).

24.4 If the Director believes that publication of any element of the Transparency Information would be contrary to the public interest, the Director shall be entitled to exclude such information from publication. The Director acknowledges that it would expect the public interest by default to be best served by publication of the Transparency Information in its entirety. Accordingly, the Director acknowledges that it will only exclude Transparency Information from publication in exceptional circumstances and agrees that where it decides to exclude information from publication it will provide a clear explanation to the Supplier.

24.5 The Director shall publish the Transparency Information in a format that assists the general public in understanding the relevance and completeness of the information being published to ensure the public obtain a fair view on how the Agreement is being performed, having regard to the context of the wider commercial relationship with the Supplier.

24.6 The Supplier agrees that any Information it holds that is not included in the Transparency Reports but is reasonably relevant to or that arises from the provision of the Services shall be provided to the Director on request unless the cost of doing so would exceed the appropriate limit prescribed under section 12 of the FOIA. The Director may disclose such information under the FOIA and the EIRs and may (except for Commercially Sensitive Information, Confidential Information (subject to Clause 23.6.3) and Open Book Data) publish such Information. The Supplier shall provide to the Director within five (5) Working Days (or such other period as the Director may reasonably specify) any such Information requested by the Director.

24.7 The Supplier acknowledges that the Director is subject to the requirements of the FOIA and the EIRs. The Supplier shall:

24.7.1 provide all necessary assistance and cooperation as reasonably requested by the Director to enable the Director to comply with its obligations under the FOIA and EIRs;

24.7.2 transfer to the Director all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within two (2) Working Days of receipt;

24.7.3 provide the Director with a copy of all Information held on behalf of the Director which is requested in a Request For Information and which is in its possession or control in the form that the Director requires within five (5) Working Days (or such other period as the Director may reasonably specify) of the Director's request for such Information; and

24.7.4 not respond directly to a Request For Information addressed to the Director unless authorised in writing to do so by the Director.

24.8 The Supplier acknowledges that the Director may be required under the FOIA and EIRs to disclose Information (including Commercially Sensitive Information) without consulting or obtaining consent from the Supplier. The Director shall take reasonable steps to notify the Supplier of a Request For Information (in accordance with the Secretary of State's section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the Director shall be responsible for determining in its absolute discretion whether any Commercially Sensitive Information and/or any other information is exempt from disclosure in accordance with the FOIA and EIRs.

25 PROTECTION OF PERSONAL DATA

Status of the Controller

25.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under this Agreement will determine the status of each Party under the Data Protection Legislation. A Party may act as:

25.1.1 "**Controller**" (where the other Party acts as the "Processor");

25.1.2 "**Processor**" (where the other Party acts as the "Controller");

and the Parties shall set out in Schedule 11 (*Processing Personal Data*) which scenario or scenarios are intended to apply under this Agreement.

Where one Party is Controller and the other Party its Processor

25.2 Where a Party is a Processor, the only processing that it is authorised to do is listed in Schedule 11 (*Processing Personal Data*) by the Controller and may not be determined by the Processor. The term "processing" and any associated terms are to be read in accordance with Article 4 of the UK GDPR and EU GDPR (as applicable).

25.3 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

25.4 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

25.4.1 a systematic description of the envisaged processing operations and the purpose of the processing;

25.4.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

25.4.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

25.4.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

25.5 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

25.5.1 process that Personal Data only in accordance with Schedule 11 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Director before processing the Personal Data unless prohibited by Law;

25.5.2 ensure that it has in place Protective Measures, including in the case of the Controller the measures set out in Clause 22 (*Director Data and Security Requirements*), which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

25.5.3 ensure that:

(a) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 11 (*Processing Personal Data*));

(b) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Processor's duties under this Clause, Clauses 23 (*Confidentiality*) and 22 (*Director Data and Security Requirements*);

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data;

25.5.4 not transfer Personal Data outside of the UK, other than to the Controller, unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(a) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR (or section 74A of DPA 2018) and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable and agreed with the Controller); or

(b) the Controller and/or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with the UK GDPR Article 46 or DPA 2018 Section 75) and/or Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:

(i) where the transfer is subject to UK GDPR:

A the UK International Data Transfer Agreement as set out in Schedule 11 (*Processing Personal Data*) or such updated version of such UK International Data Transfer Agreement as published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time***;*** or

B the European Commission's Standard Contractual Clauses per decision 2021/914/EU set out in Schedule 11 (*Processing Personal Data*) or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time ("**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**") as published by the Information Commissioner's Office from time to time; and/or

(ii) where the transfer is subject to EU GDPR, the EU SCCs,

as well as any additional measures determined by the Controller being implemented by the importing Party;

(c) the Data Subject has enforceable rights and effective legal remedies;

(d) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(e) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data; and

25.5.5 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

25.6 Subject to Clause 25.7, the Processor shall notify the Controller immediately if it:

25.6.1 receives a Data Subject Request (or purported Data Subject Request);

25.6.2 receives a request to rectify, block or erase any Personal Data;

25.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

25.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

25.6.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

25.6.6 becomes aware of a Data Loss Event.

25.7 The Processor's obligation to notify under Clause 25.6 shall include the provision of further information to the Controller in phases, as details become available.

25.8 Taking into account the nature of the processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 25.6 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

25.8.1 the Controller with full details and copies of the complaint, communication or request;

25.8.2 such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

25.8.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

25.8.4 assistance as requested by the Controller following any Data Loss Event; and/or

25.8.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

25.9 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Clause 25. This requirement does not apply where the Processor employs fewer than two hundred and fifty (250) staff, unless:

25.9.1 the Controller determines that the processing is not occasional;

25.9.2 the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

25.9.3 the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

25.10 The Processor shall allow for audits of its Data processing activity by the Controller or the Controller's designated auditor.

25.11 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

25.12 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

25.12.1 notify the Controller in writing of the intended Sub-processor and processing;

25.12.2 obtain the written consent of the Controller;

25.12.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 25 such that they apply to the Sub-processor; and

25.12.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

25.13 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

25.14 The Director may, at any time on not less than thirty (30) Working Days' notice, revise this Clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

25.15 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Director may on not less than thirty (30) Working Days' notice to the Supplier amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Standard Contractual Clauses

25.16 It is noted that on 28 June 2021 the European Commission made an implementing decision pursuant to Article 45 of the EU GDPR on the adequate protection of Personal Data by the United Kingdom which contains carve-outs for certain transfers outside of the EU to the UK of certain types of Personal Data (the "UK Adequacy Decision"). If any transfer of Personal Data which is subject to EU GDPR pursuant to this Contract is not covered by the UK Adequacy Decision or at any time during the term of the Agreement is not covered by the UK Adequacy Decision or at any time during the term of the Agreement the UK Adequacy Decision is:

25.16.1 withdrawn, invalidated, overruled or otherwise ceases to have effect; or

25.16.2 amended in such a way as to affect the transfers of Personal Data outside of the EU which are contemplated under this Agreement,

Clauses 25.17 to 25.18 shall apply.

25.17 The Parties agree:

25.17.1 that without any further action being required they have entered into the Standard Contractual Clauses in the European Commission's decision 2021/914/EU in respect of data transfers by the Supplier outside of the UK;

25.17.2 that, where no other appropriate safeguard or exemption applies, that the Personal Data subject to this Agreement (and to which Chapter V of the EU GDPR applies) will be transferred in accordance with those Standard Contractual Clauses as of the date the Parties entered into those Standard Contractual Clauses;

25.17.3 to use best endeavours to complete the annexes to the Standard Contractual Clauses promptly and at their own cost for the purpose of giving full effect to them; and

25.17.4 that if there is any conflict between this Agreement and the Standard Contractual Clauses the terms of the Standard Contractual Clauses shall apply.

25.18 In the event that the European Commission updates, amends, substitutes, adopts or publishes new Standard Contractual Clauses from time to time, the Parties agree:

25.18.1 that the most up to date Standard Contractual Clauses from time to time shall be automatically incorporated in place of those in use at the time of such update, amendment, substitution, adoption or publication and that such incorporation is not a Change;

25.18.2 that where no other appropriate safeguard or exemption applies, that the Personal Data subject to this Agreement (and to which Chapter V of the EU GDPR applies) will be transferred in accordance with the relevant form of the most up to date Standard Contractual Clauses as of the date the European Commission decision regarding such new Standard Contractual Clauses becomes effective;

25.18.3 to use best endeavours to complete any part of the most up to date Standard Contractual Clauses that a Party must complete promptly and at their own cost for the purpose of giving full effect to them; and

25.18.4 that if there is any conflict between this Agreement and the most up to date Standard Contractual Clauses the terms of the most up to date Standard Contractual Clauses shall apply.

26 PUBLICITY AND BRANDING

26.1 The Supplier shall not:

26.1.1 make any press announcements or publicise this Agreement or its contents in any way; or

26.1.2 subject to the provisions of Clause 19 and Schedule 5.2 (*Trade Mark Licence Terms*), use the Director's name or brand in any promotion or marketing or announcement of orders,

without the prior written consent of the Director, which shall not be unreasonably withheld or delayed.

26.2 Each Party acknowledges to the other that nothing in this Agreement either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Services, the Supplier System and the Director System) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

SECTION G – LIABILITY, INDEMNITIES AND INSURANCE

27 LIMITATIONS ON LIABILITY

Unlimited liability

27.1 Neither Party limits its liability for:

27.1.1 death or personal injury caused by its negligence, or that of its employees, agents or Sub-contractors (as applicable);

27.1.2 fraud or fraudulent misrepresentation by it or its employees;

27.1.3 breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Good and Services Act 1982; or

27.1.4 any liability to the extent it cannot be limited or excluded by Law.

27.2 The Supplier's liability in respect of the indemnities in Clause 10.5 (*VAT*), Clause 14.7 (*Employment Indemnity*), Clause 14.8 (*Income Tax and National Insurance Contributions*), Clause 20 (*IPRs Indemnity*), Schedule 9.1 (*Staff Transfer*) and the Annexes to Schedule 9.1 (*Staff Transfer*) shall be unlimited.

27.3 The Director's liability in respect of the indemnities in Clause 14.7 (*Employment Indemnity*), Schedule 9.1 (*Staff Transfer*) and the Annexes to Schedule 9.1 (*Staff Transfer*) shall be unlimited.

Financial and other limits

27.4 Subject to Clauses 27.1 and 27.2 (*Unlimited Liability*) and Clause 27.7 (*Consequential Losses*):

27.4.1 the Supplier's total aggregate liability in respect of loss of or damage to the Director Premises or other property or assets whether or not owned by the Director (including technical infrastructure, assets or equipment but excluding any loss or damage to the Director's Data or any other data) that is caused by Defaults of the Supplier shall in no event exceed £50,000,000 (fifty million pounds);

27.4.2 the Supplier's aggregate liability in respect of:

(a) loss or damage to Director Data; and

(b) breach of the Data Protection Legislation,

that is caused by Default of the Supplier occurring in each and any Contract Year shall in no event exceed [redacted];

27.4.3 the Supplier's aggregate liability in respect of all:

(a) Service Credits; and

(b) Compensation for Unacceptable KPI Failure,

incurred in any rolling period of twelve (12) months shall be subject to the Service Credit Cap; and

27.4.4 the Supplier's aggregate liability in respect of all other Losses incurred by the Director under or in connection with this Agreement as a result of Defaults by the Supplier shall in no event exceed:

(a) in relation to Defaults occurring in the first Contract Year, an amount equal to 150% of the Estimated Year 1 Charges;

(b) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to 150% of the Charges paid and/or due to be paid to the Supplier under this Agreement in the Contract Year immediately preceding the occurrence of the Default; and

(c) in relation to Defaults occurring after the end of the Term, an amount equal to 150% of the Charges paid and/or due to be paid to the Supplier in the twelve (12) month period immediately prior to the last day of the Term,

provided that where any Losses referred to in this Clause 27.4.4 have been incurred by the Director as a result of the Supplier's abandonment of this Agreement or the Supplier's wilful default, wilful breach of a fundamental term of this Agreement or wilful repudiatory breach of this Agreement, the references in such Clause to 150% shall be deemed to be references to 200%.

27.5 Deductions from Charges shall not be taken into consideration when calculating the Supplier's liability under Clause 27.4.3.

27.6 Subject to Clauses 27.1 and 27.3 (*Unlimited Liability*) and Clause 27.7 (*Consequential Losses*) and without prejudice to the Director's obligation to pay the Charges as and when they fall due for payment:

27.6.1 the Director's total aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Agreement as a result of early termination of this Agreement by the Director pursuant to Clause 35.1.1 (*Termination by the Director*) or by the Supplier pursuant to Clause 35.3 (*Termination by the Supplier*) shall in no event exceed the following amounts:

(a) in relation to the Breakage Costs Payment, the amount set out in Paragraph 3.2 of Schedule 7.2 (*Payments on Termination*); and

(b) in relation to the Compensation Payment, the amount set out in Paragraph 5 of Schedule 7.2 (*Payments on Termination*); and

27.6.2 the Director's aggregate liability in respect of all Losses incurred by the Supplier under or in connection with this Agreement as a result of Defaults of the Director shall in no event exceed:

(a) in relation to Defaults occurring in the first Contract Year, an amount equal to the Estimated Year 1 Charges;

(b) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to the total Charges paid and/or due to be paid under this Agreement in the Contract Year immediately preceding the occurrence of the Default; and

(c) in relation to Defaults occurring after the end of the Term, an amount equal to the total Charges paid and/or due to be paid to the Supplier in the twelve (12) month period immediately prior to the last day of the Term.

Consequential Losses

27.7 Subject to Clauses 27.1, 27.2 and 27.3 (*Unlimited Liability*) and Clause 27.8, neither Party shall be liable to the other Party for:

27.7.1 any indirect, special or consequential Loss; or

27.7.2 any loss of profits or turnover (in each case whether direct or indirect).

27.8 Notwithstanding Clause 27.7 but subject to Clause 27.4, the Supplier acknowledges that the Director may, amongst other things, recover from the Supplier the following Losses incurred by the Director to the extent that they arise as a result of a Default by the Supplier:

27.8.1 any additional operational and/or administrative costs and expenses suffered or incurred by the Director, including costs relating to time spent by or on behalf of the Director in dealing with the consequences of the Default under this Agreement and/or the Collaboration Agreement (which may include those costs incurred by a Relevant Third Party Supplier);

27.8.2 any wasted expenditure or charges;

27.8.3 the additional cost of procuring Replacement Services for the remainder of the Term and/or replacement Deliverables, which shall include any incremental costs associated with such Replacement Services and/or replacement Deliverables above those which would have been payable under this Agreement;

27.8.4 not used;

27.8.5 any compensation or interest paid to a third party by or on behalf of the Director including:

(a) payments to Customers for reimbursement of Customer funds;

(b) payments made in accordance with the Director's Compensation and Goodwill Policy; and

(c) payments or fines imposed by a regulatory body including the Financial Services Ombudsman or the Information Commissioners Office,

save where such Losses arise from an incorrect instruction issued by the Director;

27.8.6 Customer overpayments save where such loss arises from an incorrect instruction issued by the Director;

27.8.7 any fine or penalty incurred by the Director pursuant to Law and any costs incurred by the Director in defending any proceedings which result in such fine or penalty;

27.8.8 Losses arising from any loss or corruption of data, including the costs of reconstituting such lost or corrupted data; and

27.8.9 advertising costs or other communication costs reasonably incurred to limit damage caused to the reputation or integrity of the Director or any Product arising out of a Default of the Supplier.

Conduct of indemnity claims

27.9 Where under this Agreement one Party indemnifies the other Party, the Parties shall comply with the provisions of Schedule 8.7 (*Conduct of Claims*) in relation to the conduct of claims made by a third person against the Party having (or claiming to have) the benefit of the indemnity.

Mitigation

27.10 Each Party shall use all reasonable endeavours to mitigate any loss or damage suffered arising out of or in connection with this Agreement, including any Losses for which the relevant Party is entitled to bring a claim against the other Party pursuant to the indemnities in this Agreement.

28 INSURANCE

28.1 The Supplier shall comply with the provisions of Schedule 2.5 (*Insurance Requirements*) in relation to obtaining and maintaining insurance.

SECTION H – REMEDIES AND RELIEF

29 RECTIFICATION PLAN PROCESS

29.1 In the event that:

29.1.1 there is, or, in the Director's opinion is reasonably likely to be, a Delay; and/or

29.1.2 in any Service Period there has been:

(a) a Material KPI Failure; and/or

(b) a Material PI Failure; and/or

29.1.3 the Supplier commits or in the Director's opinion is reasonably likely to commit, a Default (including, without limitation, obligations set out in Schedule 7.6 (*Regulatory, Compliance and Financial Crime*)) that has or may have an adverse effect on the provision of the Services or the ability of the Director to fulfil its obligations (contractual, regulatory and/or statutory) that is capable of remedy;

29.1.4 the Supplier commits or in the Director's opinion is reasonably likely to commit, a Default that has or may have an adverse effect on the provision of the services to be provided by any Relevant Third Party Supplier that is capable of remedy;

29.1.5 the Supplier fails to comply or in the Director's opinion is reasonably likely to fail to comply, with any of its obligations under the Collaboration Agreement (including, without limitation, its obligations in Clauses 5, 6 and 7) which the Director considers, acting reasonably, has an adverse impact including Delay on the provision of any of the Services of the Supplier or adverse impact on any Relevant Third Party Supplier; or

29.1.6 the Supplier becomes aware of a failure by any Relevant Third Party Supplier or the Director which may lead to a Supplier or Director Default,

(each a "**Notifiable Default**"), then the Supplier shall notify the Director of the Notifiable Default as soon as practicable, but in any event within two (2) Working Days of becoming aware (including following a notification from the Director) of the Notifiable Default. Such notification from the Supplier shall detail the actual or anticipated effect of the Notifiable Default on itself, the Relevant Third Party Suppliers and the Director. Unless the Notifiable Default also constitutes a Rectification Plan Failure or other Supplier Termination Event, the Director may not terminate this Agreement in whole or in part on the grounds of the Notifiable Default without first following the Rectification Plan Process. Where the Notifiable Default relates to the acts or omissions of the Relevant Third Party Suppliers, the Supplier must still comply with its obligation to notify the Director under this Clause 29.1 (and, if applicable, any other notification obligation under the Collaboration Agreement), and in such situation the Director shall determine whether a Rectification Plan Process is appropriate on a case-by-case basis.

Notification

29.2 If:

29.2.1 the Supplier notifies the Director pursuant to Clause 29.1 that a Notifiable Default has occurred; or

29.2.2 the Director becomes aware of the Notifiable Default before the Supplier has notified the Director pursuant to Clause 29.1, the Director may notify the Supplier that it considers that a Notifiable Default has occurred (setting out detail of the matter and what the Supplier has to rectify),

then the Supplier shall comply with the Rectification Plan Process, provided that Clause 29.2 shall not apply where the Notifiable Default also constitutes a Supplier Termination Event and the Director serves a Termination Notice and the Parties agree that the Notifiable Default could not be rectified before the Termination Notice expires.

29.3 For the avoidance of doubt, the Supplier shall still have an obligation to mitigate and, where possible, rectify Notifiable Defaults during the Term of the Agreement regardless of the Rectification Plan Process being followed.

29.4 If the Supplier does not notify the Director pursuant to Clause 29.1 that a Notifiable Default has occurred, without prejudice to the Director's right to notify the Supplier under Clause 29.2, or the Notifiable Default is irremediable then the Director may, as soon as becoming aware of the Notifiable Default, terminate this Agreement in whole or in part by a Termination Notice to the Supplier on the grounds of the Notifiable Default without first following the Rectification Plan Process.

Submission of the draft Rectification Plan

29.5 The Supplier shall submit a draft Rectification Plan to the Director for it to review as soon as possible and in any event within ten (10) Working Days (or such other period as may be agreed between the Parties but noting the Parties are not obliged to agree any extension) after the date of the original notification pursuant to Clause 29.2 (*Notification*). The Supplier shall submit a draft Rectification Plan to the Director even if the Supplier disputes that it is responsible for the Notifiable Default.

29.6 The draft Rectification Plan issued pursuant to Clause 29.5 or Clause 29.8 shall set out as a minimum:

29.6.1 full details of the Notifiable Default that has occurred, including a root cause analysis;

29.6.2 the actual or anticipated effect of the Notifiable Default, including the effect on Relevant Third Party Suppliers and the Director;

29.6.3 the steps which the Supplier proposes to take to rectify the Notifiable Default and to prevent such Notifiable Default from recurring, including timescales for such steps and, for the rectification of the Notifiable Default; and

29.6.4 any Dependencies the Supplier has on the Director or Relevant Third Party Suppliers to enable the Supplier to remedy the Notifiable Default (if any).

29.7 The Supplier shall promptly provide to the Director any further documentation that the Director reasonably requires to assess the Supplier's root cause analysis and/or other draft Rectification Plan details. If the Parties do not agree on the root cause and/or any other Rectification Plan detail set out in the draft Rectification Plan, the Director can reject the draft Rectification Plan in accordance with Clause 29.10.

29.8 Where the root cause analysis identifies the root cause to be with a Relevant Third Party Supplier, the Supplier shall immediately notify the Director on becoming aware of this and the Director shall, at its sole discretion, either:

29.8.1 agree and cancel the Notifiable Default notice;

29.8.2 require the Supplier to work jointly with the Relevant Third Party Supplier(s) to develop a joint Rectification Plan in accordance with this Clause 29; or

29.8.3 reject the root cause finding and require the Supplier continues to produce a Draft Rectification Plan in accordance with Clause 29.6.

29.9 Where the Director requires, the Supplier shall work in good faith with one or more Relevant Third Party Suppliers in preparing a draft Rectification Plan notwithstanding that there has not been a Notifiable Default initiated under this Clause 29.

Agreement of the Rectification Plan

29.10 The Director may reject the draft Rectification Plan by notice to the Supplier if it considers that the draft Rectification Plan is inadequate, for example because the draft Rectification Plan:

29.10.1 is insufficiently detailed to be capable of proper evaluation;

29.10.2 will take too long to complete;

29.10.3 will not prevent reoccurrence of the Notifiable Default;

29.10.4 will rectify the Notifiable Default but in a manner which is unacceptable to the Director; or

29.10.5 does not provide the information required pursuant to Clause 29.6.

29.11 The Director shall notify the Supplier whether it consents to the draft Rectification Plan as soon as reasonably practicable. If the Director rejects the draft Rectification Plan pursuant to Clause 29.10, the

Director shall give reasons for its decision and the Supplier shall resolve the Director's reasons in the preparation of a revised Rectification Plan. The right to revise the draft Rectification Plan shall only apply on the first submission of such a draft Rectification Plan. The Supplier shall submit the first revised draft of the Rectification Plan to the Director for review within five (5) Working Days (or such other period as agreed between the Parties but noting the Parties are not obliged to agree any extension) of the date of the Director's notice rejecting the first draft.

29.12 On receipt of the revised draft Rectification Plan pursuant to Clause 29.11, the Director shall undertake a further review in accordance with Clause 29.10, to be escalated and undertaken by an individual of appropriate seniority. In the event that, following the further review, the Director rejects the revised draft Rectification Plan, the Director may, in its sole discretion:

29.12.1 permit the Supplier to further revise the draft Rectification Plan, in which case the terms of Clause 29.11 shall apply, save that the review shall be further escalated to and undertaken by a sufficiently senior level of management; or

29.12.2 terminate this Agreement in whole or in part by a Termination Notice to the Supplier.

29.13 If the Director consents to the draft Rectification Plan, this shall become the agreed Rectification Plan and:

29.13.1 the Supplier shall immediately start work on the actions set out in the Rectification Plan;

29.13.2 the Director may no longer terminate this Agreement in whole or in part on the grounds of the relevant Notifiable Default save in the event of a Rectification Plan Failure or other Supplier Termination Event; and

29.13.3 all costs:

(a) incurred by the Supplier; or

(b) reasonably incurred and evidenced by Relevant Third Party Suppliers and the Director in supporting the delivery of a Rectification Plan Process, where the Notifiable Default originated with the Supplier,

shall be borne by the Supplier.

30 NOT USED

31 REMEDIAL ADVISER

31.1 If:

31.1.1 any of the Intervention Trigger Events occur; or

31.1.2 the Director believes that any of the Intervention Trigger Events have occurred or are likely to occur,

(each an "**Intervention Cause**"), the Director may give notice to the Supplier (an "**Intervention Notice**") giving details of the Intervention Cause and requiring:

31.1.3 a meeting between the Director Representative and the Supplier Representative and, where appropriate, Relevant Third Party Supplier representatives, to discuss the Intervention Cause; and

31.1.4 where the Director requires a Remedial Adviser to be appointed, the appointment as soon as practicable by the Supplier of a Remedial Adviser, as further described in this Clause 31.

For the avoidance of doubt, if the Intervention Cause is also a Supplier Termination Event, the Director has no obligation to exercise its rights under this Clause 31.1 prior to or instead of exercising its right to terminate this Agreement.

If the Supplier fails to attend the meeting in accordance with the notice given by the Director under Clause 31.1, the Supplier will automatically be obligated to appoint a Remedial Adviser in accordance with this Clause 31 regardless of whether the notice required such appointment or not.

31.2 If the Director gives notice that it requires the appointment of a Remedial Adviser:

31.2.1 the Remedial Adviser shall be:

(a) a person selected by the Supplier and approved by the Director; or

(b) if none of the persons selected by the Supplier have been approved by the Director (or no person has been selected by the Supplier) within ten (10) Working Days following the date on which the Intervention Notice is deemed served, a person identified by the Director;

31.2.2 the terms of engagement agreed with the Remedial Adviser must be approved by the Director; and

31.2.3 the Remedial Adviser start date within the terms of engagement shall be a date specified by the Director; and

31.2.4 any right of the Director to terminate this Agreement pursuant to Clause 35.1.2 (*Termination by the Director*) for the occurrence of that Intervention Cause shall be suspended for sixty (60) Working Days from (and including) the date of the Intervention Notice (or such other period as may be agreed between the Parties but noting the Parties are not obliged to agree any extension) (the "**Intervention Period**").

31.3 The Remedial Adviser's overall objective shall be to advise the Supplier and provide recommendations to the Supplier of how to mitigate the effects of, and (to the extent capable of being remedied) to recommend steps to remedy, the Intervention Cause and to avoid the occurrence of similar circumstances in the future. In furtherance of this objective (but without diminishing the Supplier's responsibilities under this Agreement), the Parties agree that the Remedial Adviser may undertake any one or more of the following actions:

31.3.1 observe the conduct of and work alongside the Supplier Personnel to the extent that the Remedial Adviser considers reasonable and proportionate having regard to the Intervention Cause;

31.3.2 gather any information the Remedial Adviser considers relevant in the furtherance of its objective;

31.3.3 write reports and provide information to the Director in connection with the steps being taken by the Supplier to remedy the Intervention Cause;

31.3.4 make recommendations to the Director and/or the Supplier as to how the Intervention Cause might be remedied and mitigated or avoided in the future; and/or

31.3.5 any other steps that the Director and/or the Remedial Adviser reasonably considers necessary or expedient in order to mitigate or rectify the Intervention Cause,

provided that any recommendations shall be subject to the Director's approval prior to being adopted.

31.4 During the Remedial Adviser's appointment the Supplier shall support and co-operate with the Remedial Adviser including, without limitations:

31.4.1 work alongside, provide information to, co-operate in good faith with and adopt any methodology in providing the Services recommended by the Remedial Adviser; and

31.4.2 ensure that the Remedial Adviser has all the access it may require in order to carry out its objective, including access to the Assets.

31.5 Following the Director's approval, the Supplier shall comply with the recommendations made by the Remedial Adviser including by, without limitations:

31.5.1 implementing such additional monitoring as the Director and/or the Remedial Adviser considers reasonable and proportionate in respect of the Intervention Cause;

31.5.2 implementing any recommendations made by the Remedial Adviser (such recommendations to be practicable and proportionate in the circumstances for the Supplier to adopt) that have been approved by the Director within the timescales given by the Remedial Adviser; and

31.5.3 engaging and co-operating with the Relevant Third Party Suppliers to accommodate the Remedial Adviser's recommendations.

31.6 Where the Director does not provide its approval of the Remedial Adviser's recommendations in accordance with Clause 31.3 the following steps shall be followed:

31.6.1 the Director shall give notice to the Remedial Adviser of its reasoning for not approving the recommendations and, at the Director's sole discretion, the Director may include suggested changes within the notice;

31.6.2 the Remedial Adviser shall then have five (5) Working Days to revise its recommendations taking into consideration the Director's reasons provided under Clause 31.6.1 before resubmitting to the Director for approval; and

31.6.3 if the Director still does not approve of the recommendations, the Director (at its complete discretion) may either:

(a) request the resubmission of further revised recommendations in accordance with Clause 31.6.2; or

(b) inform the Supplier to terminate the Remedial Adviser's appointment and appoint a new Remedial Adviser in accordance with Clause 31.2.

31.7 The Supplier shall not terminate the appointment of the Remedial Adviser prior to the end of the Intervention Period without the prior consent of the Director (such consent not to be unreasonably withheld).

31.8 The Supplier shall be responsible for:

31.8.1 the costs of appointing, and the fees charged by, the Remedial Adviser; and

31.8.2 its own costs and those reasonably incurred and evidenced by Relevant Third Party Suppliers in connection with any action required by the Director and/or the Remedial Adviser pursuant to this Clause 31.

31.9 If:

31.9.1 the Supplier:

(a) fails to perform any of the steps in this Clause 31 or otherwise required by the Director in an Intervention Notice; and/or

(b) is in Default of any of its obligations under Clause 31.4; and/or

31.9.2 the relevant Intervention Trigger Event is not rectified by the end of the Intervention Period,

(each a "**Remedial Adviser Failure**"), the Director shall be entitled to terminate this Agreement pursuant to Clause 35.1.2 (*Termination by the Director*).

32 STEP-IN RIGHTS

32.1 On the occurrence of a Step-In Trigger Event, the Director may serve notice on the Supplier (a "**Step-In Notice**") that it will be taking action under this Clause 32 (*Step-in Rights*), either itself or with the assistance of a third party (provided that the Supplier may require any third parties to comply with a confidentiality undertaking equivalent to Clause 23 (*Confidentiality*)). The Step-In Notice shall set out the following:

32.1.1 the action the Director wishes to take and in particular the Services that it wishes to control (the "**Required Action**");

32.1.2 the Step-In Trigger Event that has occurred and whether the Director believes that the Required Action is due to the Supplier's Default;

32.1.3 the date on which it wishes to commence the Required Action;

32.1.4 the time period which it believes will be necessary for the Required Action;

32.1.5 whether the Director will require access to the Supplier's premises and/or the Sites; and

32.1.6 to the extent practicable, the impact that the Director anticipates the Required Action will have on the Supplier's obligations to provide the Services during the period that the Required Action is being taken.

32.2 Following service of a Step-In Notice, the Director shall:

32.2.1 take the Required Action set out in the Step-In Notice and any consequential additional action as it reasonably believes is necessary to achieve the Required Action;

32.2.2 keep records of the Required Action taken and provide information about the Required Action to the Supplier;

32.2.3 co-operate wherever reasonable with the Supplier in order to enable the Supplier to continue to provide the Services in relation to which the Director is not assuming control; and

32.2.4 act reasonably in mitigating the cost that the Supplier will incur as a result of the exercise of the Director's rights under this Clause 32.

32.3 For so long as and to the extent that the Required Action is continuing, then:

32.3.1 the Supplier shall not be obliged to provide the Services to the extent that they are the subject of the Required Action;

32.3.2 no Deductions shall be applicable in relation to Charges in respect of Services that are the subject of the Required Action and the provisions of Clause 32.4 shall apply to Deductions from Charges in respect of other Services; and

32.3.3 the Director shall pay to the Supplier the Charges after subtracting any applicable Deductions and the Director's costs of taking the Required Action.

32.4 If the Supplier demonstrates to the reasonable satisfaction of the Director that the Required Action has resulted in:

32.4.1 the degradation of any Services not subject to the Required Action; or

32.4.2 the non-Achievement of a Milestone,

beyond that which would have been the case had the Director not taken the Required Action, then the Supplier shall be entitled to an agreed adjustment of the Charges.

32.5 Before ceasing to exercise its step in rights under this Clause 32 the Director shall deliver a written notice to the Supplier (a "**Step-Out Notice**"), specifying:

32.5.1 the Required Action it has actually taken; and

32.5.2 the date on which the Director plans to end the Required Action (the "**Step-Out Date**") subject to the Director being satisfied with the Supplier's ability to resume the provision of the Services and the Supplier's plan developed in accordance with Clause 32.6.

32.6 The Supplier shall, following receipt of a Step-Out Notice and not less than twenty (20) Working Days prior to the Step-Out Date, develop for the Director's approval a draft plan (a "**Step-Out Plan**") relating to the resumption by the Supplier of the Services, including any action the Supplier proposes to take to ensure that the affected Services satisfy the requirements of this Agreement.

32.7 If the Director does not approve the draft Step-Out Plan, the Director shall inform the Supplier of its reasons for not approving it. The Supplier shall then revise the draft Step-Out Plan taking those reasons into account and shall re-submit the revised plan to the Director for the Director's approval. The Director shall not withhold or delay its approval of the draft Step-Out Plan unnecessarily.

32.8 The Supplier shall bear its own costs in connection with any step-in by the Director under this Clause 32, provided that the Director shall reimburse the Supplier's reasonable additional expenses incurred directly as a result of any step-in action taken by the Director under:

32.8.1 limbs (c) or (d) of the definition of a Step-In Trigger Event; or

32.8.2 limbs (e) and (f) of the definition of a Step-in Trigger Event (insofar as the primary cause of the Director serving the Step-In Notice is identified as not being the result of the Supplier's Default).

33 DIRECTOR CAUSE

33.1 Notwithstanding any other provision of this Agreement, if the Supplier has failed to:

33.1.1 Achieve a Milestone by its Milestone Date;

33.1.2 provide the Operational Services in accordance with the Target Performance Levels; and/or

33.1.3 comply with its obligations under this Agreement,

(each a "**Supplier Non-Performance**"), and can demonstrate that the Supplier Non-Performance would not have occurred but for a Director Cause, then (subject to the Supplier fulfilling its obligations in this Clause 33):

33.1.4 the Supplier shall not be treated as being in breach of this Agreement to the extent the Supplier can demonstrate that the Supplier Non-Performance was caused by the Director Cause;

33.1.5 the Director shall not be entitled to exercise any rights that may arise as a result of that Supplier Non-Performance:

(a) to terminate this Agreement pursuant to Clause 35.1.2 (*Termination by the Director*); or

(b) to take action pursuant to Clause 31 (*Remedial Adviser*) or Clause 32 (*Step-In Rights*);

33.1.6 where the Supplier Non-Performance constitutes the failure to Achieve a Milestone by its Milestone Date:

(a) the Milestone Date shall be postponed by a period equal to the period of Delay that the Supplier can demonstrate was solely caused by the Director Cause;

(b) if the Director, acting reasonably, considers it appropriate, the Implementation Plan shall be amended to reflect any consequential revisions required to subsequent Milestone Dates resulting from the Director Cause; and

(c) the Supplier shall be entitled to claim compensation subject to and in accordance with the principles set out in Paragraph 2 of Part 3 of Schedule 7.1 (*Charges and Invoicing*); and/or

33.1.7 where the Supplier Non-Performance constitutes a Performance Failure:

(a) the Supplier shall not be liable to accrue Service Credits;

(b) the Director shall not be entitled to withhold any of the Service Charges pursuant to Clause 7.2.4(b) (*Performance Failures*);

(c) the Director shall not be entitled to withhold and retain any Compensation for Unacceptable KPI Failure pursuant to Clause 7.3.1 (*Unacceptable KPI Failure*); and

(d) the Supplier shall be entitled to invoice for the Service Charges for the relevant Operational Services affected by the Director Cause,

in each case, to the extent that the Supplier can demonstrate that the Performance Failure was caused by the Director Cause.

33.2 In order to claim any of the rights and/or relief referred to in Clause 33.1, the Supplier shall as soon as reasonably practicable (and in any event within five (5) Working Days) after becoming aware that a Director Cause has caused, or is reasonably likely to cause, a Supplier Non-Performance, give the Director notice (a "**Relief Notice**") setting out details of:

33.2.1 the Supplier Non-Performance;

33.2.2 the Director Cause and its effect, or likely effect, on the Supplier's ability to meet its obligations under this Agreement;

33.2.3 any steps which the Director can take to eliminate or mitigate the consequences and impact of such Director Cause; and

33.2.4 the relief and/or compensation claimed by the Supplier.

33.3 The Supplier's failure to deliver the Relief Notice to the Director in accordance with Clause 33.2 shall constitute a waiver of this Clause 33 and the Supplier's rights under it including the Supplier's entitlement to relief and/or compensation.

33.4 Following the receipt of a Relief Notice, the Director shall as soon as reasonably practicable consider the nature of the Supplier Non-Performance and the alleged Director Cause and whether it agrees with the Supplier's assessment set out in the Relief Notice as to the effect of the relevant Director Cause and its entitlement to relief and/or compensation, consulting with the Supplier where necessary.

33.5 The Supplier shall use all reasonable endeavours to eliminate or mitigate the consequences and impact of any Director Cause, including any Losses that the Supplier may incur and the duration and consequences of any Delay or anticipated Delay.

33.6 Without prejudice to Clause 5.10 (*Continuing obligation to provide the Services*), if a Dispute arises as to:

33.6.1 whether a Supplier Non-Performance would not have occurred but for a Director Cause; and/or

33.6.2 the nature and/or extent of the relief and/or compensation claimed by the Supplier,

either Party may refer the Dispute to the Dispute Resolution Procedure. Pending the resolution of the Dispute, both Parties shall continue to resolve the causes of, and mitigate the effects of, the Supplier Non-Performance.

33.7 Any Change that is required to the Implementation Plan or to the Charges pursuant to this Clause 33 shall be implemented in accordance with the Change Control Procedure.

34 FORCE MAJEURE

34.1 Subject to the remaining provisions of this Clause 34 (and, in relation to the Supplier, subject to its compliance with its obligations in Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*)), a Party may claim relief under this Clause 34 from liability for failure to meet its obligations under this Agreement for as long as and only to the extent that the performance of those obligations is directly affected by a Force Majeure Event. Any failure or delay by the Supplier in performing its obligations under this Agreement which results from a failure or delay by an agent, Sub-contractor or supplier shall be regarded as due to a Force Majeure Event only if that agent, Sub-contractor or supplier is itself impeded by a Force Majeure Event from complying with an obligation to the Supplier.

34.2 The Affected Party shall as soon as reasonably practicable issue a Force Majeure Notice, which shall include details of the Force Majeure Event, its effect on the obligations of the Affected Party and any action the Affected Party proposes to take to mitigate its effect.

34.3 If the Supplier is the Affected Party, it shall not be entitled to claim relief under this Clause 34 to the extent that consequences of the relevant Force Majeure Event:

34.3.1 are capable of being mitigated, but the Supplier has failed to do so;

34.3.2 should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by this Agreement; or

34.3.3 are the result of the Supplier's failure to comply with its Service Continuity Plan (except to the extent that such failure is also due to a Force Majeure Event that affects the execution of the Service Continuity Plan).

34.4 Subject to Clause 34.5, as soon as practicable after the Affected Party issues the Force Majeure Notice, and at regular intervals thereafter, the Parties shall consult in good faith and use reasonable endeavours to agree any steps to be taken and an appropriate timetable in which those steps should be taken, to enable continued provision of the Services affected by the Force Majeure Event.

34.5 The Parties shall at all times following the occurrence of a Force Majeure Event and during its subsistence use their respective reasonable endeavours to prevent and mitigate the effects of the Force Majeure Event. Where the Supplier is the Affected Party, it shall take all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Force Majeure Event.

34.6 Where, as a result of a Force Majeure Event:

34.6.1 an Affected Party fails to perform its obligations in accordance with this Agreement, then during the continuance of the Force Majeure Event:

(a) the other Party shall not be entitled to exercise any rights to terminate this Agreement in whole or in part as a result of such failure other than pursuant to Clause 35.1.3 (*Termination by the Director*); and

(b) neither Party shall be liable for any Default arising as a result of such failure; and/or

34.6.2 the Supplier fails to perform its obligations in accordance with this Agreement:

(a) the Director shall not be entitled:

(i) during the continuance of the Force Majeure Event to exercise its rights under Clause 31 (*Remedial Adviser*) and/or Clause 32 (*Step-in Rights*) as a result of such failure;

(ii) to receive Service Credits, to withhold any of the Service Charges pursuant to Clause 7.2.4(b) (*Performance Failures*) or withhold and retain any of the Service Charges as compensation pursuant to Clause 7.3.1 (*Unacceptable KPI Failure*) to the extent that a Performance Failure has been caused by the Force Majeure Event; and

(b) the Supplier shall be entitled to receive payment of the Charges (or a proportional payment of them) only to the extent that the Services (or part of the Services) continue to be performed in accordance with the terms of this Agreement during the occurrence of the Force Majeure Event.

34.7 The Affected Party shall notify the other Party as soon as practicable after the Force Majeure Event ceases or no longer causes the Affected Party to be unable to comply with its obligations under this Agreement.

34.8 Relief from liability for the Affected Party under this Clause 34 shall end as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under this Agreement and shall not be dependent on the serving of notice under Clause 34.7.

SECTION I – TERMINATION AND EXIT MANAGEMENT

35 TERMINATION RIGHTS

Termination by the Director

35.1 The Director may terminate this Agreement by issuing a Termination Notice to the Supplier:

35.1.1 for convenience at any time, including where the Agreement should not have been entered into in view of a serious infringement of obligations under the Public Contracts Regulations 2015;

35.1.2 if a Supplier Termination Event occurs;

35.1.3 if a Force Majeure Event endures for a continuous period of more than ninety (90) days; or

35.1.4 if the Agreement has been substantially amended to the extent that the Public Contracts Regulations 2015 require a new procurement procedure,

and this Agreement shall terminate on the date specified in the Termination Notice.

35.2 Where the Director:

35.2.1 is terminating this Agreement under Clause 35.1.2 due to the occurrence of either limb (b) and/or (g) of the definition of Supplier Termination Event, it may rely on a single material Default or on a number of Defaults or repeated Defaults (whether of the same or different obligations and regardless of whether such Defaults are cured) which taken together constitute a material Default; and/or

35.2.2 has the right to terminate this Agreement under Clauses 35.1.1 to 35.1.3, it may, prior to or instead of terminating the whole of this Agreement, serve a Termination Notice requiring the partial termination of this Agreement to the extent identified in the Termination Notice.

Termination by the Supplier

35.3 The Supplier may, by issuing a Termination Notice to the Director, terminate this Agreement if the Director fails to pay an undisputed sum due to the Supplier under this Agreement which in aggregate exceeds [redacted] and such amount remains outstanding forty (40) Working Days after the receipt by the Director of a notice of non-payment from the Supplier.

35.4 This Agreement or the relevant Services (as the case may be) shall then terminate on the date specified in the Termination Notice (which shall not be less than twenty (20) Working Days from the date of the issue of the Termination Notice).

Partial Termination

35.5 If the Supplier notifies the Director pursuant to Clause 35.3 (*Termination by the Supplier*) that it intends to terminate this Agreement in part and the Director, acting reasonably, believes that the effect of such Partial Termination is to render the remaining Services incapable of meeting a significant part of the Director Requirements, then the Director shall be entitled to terminate the remaining part of this Agreement by serving a Termination Notice to the Supplier within one (1) month of receiving the Supplier's Termination Notice. For the purpose of this Clause 35.5, in assessing the significance of any part of the Director Requirements, regard shall be had not only to the proportion of that part to the Director Requirements as a whole, but also to the importance of the relevant part to the Director.

35.6 The Parties shall agree the effect of any Change necessitated by a Partial Termination in accordance with the Change Control Procedure, including the effect the Partial Termination may have on any other Services and the Charges, provided that:

35.6.1 the Supplier shall not be entitled to an increase in the Charges in respect of the Services that have not been terminated if the Partial Termination arises due to the occurrence of a Supplier Termination Event;

35.6.2 any adjustment to the Charges (if any) shall be calculated in accordance with the Financial Model and must be reasonable; and

35.6.3 the Supplier shall not be entitled to reject the Change.

36 CONSEQUENCES OF EXPIRY OR TERMINATION

General Provisions on Expiry or Termination

36.1 The provisions of Clauses 5.9 (*Specially Written Software warranty*), 10.4 and 10.5 (*VAT*), 10.6 and 10.7 (*Set-off and Withholding*), 12 (*Records, Reports, Audits & Open Book Data*), 14.7 (*Employment Indemnity*), 14.8 (*Income Tax and National Insurance Contributions*), 16 (*Intellectual Property Rights*), 17 (*Transfer and Licences Granted by the Supplier*), 20.1 (*IPRs Indemnity*), 23 (*Confidentiality*), 24 (*Transparency and Freedom of Information*), 25 (*Protection of Personal Data*), 27 (*Limitations on Liability*), 36 (*Consequences of Expiry or Termination*), 43 (*Severance*), 45 (*Entire Agreement*), 46 (*Third Party Rights*), 48 (*Disputes*) and 49 (*Governing Law and Jurisdiction*), and the provisions of Schedules 1 (*Definitions*), 7.1 (*Charges and Invoicing*), 7.2 (*Payments on Termination*), 7.5 (*Financial*

Reports, Audit and Risk), 8.3 (*Dispute Resolution Procedure*), 8.4 (*Reports and Records Provisions*), 8.5 (*Exit Management*), and 9.1 (*Staff Transfer*), shall survive the termination or expiry of this Agreement.

Exit Management

36.2 The Parties shall comply with the provisions of Schedule 8.5 (*Exit Management*) and any current Exit Plan in relation to orderly transition of the Services to the Director or a Replacement Supplier.

Payments by the Director

36.3 If this Agreement is terminated by the Director pursuant to Clause 35.1.1 (*Termination by the Director*) or by the Supplier pursuant to Clause 35.3 (*Termination by the Supplier*), the Director shall pay the Supplier the following payments (which shall be the Supplier's sole remedy for the termination of this Agreement):

36.3.1 the Termination Payment; and

36.3.2 the Compensation Payment, if either of the following periods is twelve (12) months or less:

(a) the period from (but excluding) the date that the Termination Notice is given (or, where Paragraph 2.1.4 of Part 4 of Schedule 7.1 (*Charges and Invoicing*) applies, deemed given) by the Director pursuant to Clause 35.1.1 (*Termination by the Director*) to (and including) the Termination Date; or

(b) the period from (and including) the date of the non-payment by the Director referred to in Clause 35.3 (*Termination by the Supplier*) to (and including) the Termination Date.

36.4 If this Agreement is terminated (in part or in whole) by the Director pursuant to Clauses 35.1.2, 35.1.3 and/or 35.2 (*Termination by the Director*), or the Term expires, the only payments that the Director shall be required to make as a result of such termination (whether by way of compensation or otherwise) are:

36.4.1 payments in respect of any Assets or apportionments in accordance with Schedule 8.5 (*Exit Management*); and

36.4.2 payments in respect of unpaid Charges for Services received up until the Termination Date.

36.5 The costs of termination incurred by the Parties shall lie where they fall if:

36.5.1 the Director terminates or partially terminates this Agreement for a continuing Force Majeure Event pursuant to Clauses 35.1.3 or 35.2.2 (*Termination by the Director*); or

36.5.2 the Director terminates this Agreement under Clause 35.1.4 (*Termination by the Director*).

Payments by the Supplier

36.6 In the event of termination or expiry of this Agreement, the Supplier shall repay to the Director all Charges it has been paid in advance in respect of Services not provided by the Supplier as at the date of expiry or termination.

36.7 If this Agreement is terminated by the Director before the Operational Services Commencement Date pursuant to Clause 35.1.2 (*Termination by the Director*) the Director shall have the right to:

36.7.1 retain all and any Deliverables which have been paid for in accordance with the Agreement and which have been supplied prior to the date of termination; and

36.7.2 recover any Charges paid in respect of the Implementation Services including Charges paid in respect of Achieved Milestones and Deliverables, less the value of any Deliverables being retained pursuant to Clause 36.7.1.

36.8 For the purpose of Clause 36.7, the value of the Retained Deliverables shall be determined by reference to the Financial Model and failing this method, through Expert Determination in accordance with Schedule 8.3 (*Dispute Resolution Procedure*).

SECTION J – MISCELLANEOUS AND GOVERNING LAW

37 COMPLIANCE

Health and Safety

37.1 The Supplier shall perform its obligations under this Agreement (including those in relation to the Services) in accordance with:

37.1.1 all applicable Law regarding health and safety; and

37.1.2 the Health and Safety Policy whilst at the Director Premises.

37.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Director Premises of which it becomes aware and which relate to or arise in connection with the performance of this Agreement. The Supplier shall instruct the Supplier Personnel to adopt any necessary associated safety measures in order to manage any such material health and safety hazards.

Equality and Diversity

37.3 The Supplier shall:

37.3.1 perform its obligations under this Agreement (including those in relation to the Services) in accordance with:

(a) all applicable equality Laws (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy, maternity or otherwise);

(b) the Director's equality and diversity policy as provided to the Supplier from time to time; and

(c) any other requirements and instructions which the Director reasonably imposes in connection with any equality obligations imposed on the Director at any time under applicable equality Law; and

37.3.2 take all necessary steps, and inform the Director of the steps taken, to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission or (any successor organisation).

Official Secrets Act and Finance Act

37.4 The Supplier shall comply with the provisions of:

37.4.1 the Official Secrets Acts 1911 to 1989; and

37.4.2 section 182 of the Finance Act 1989.

38 ASSIGNMENT AND NOVATION

38.1 The Supplier shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Director.

38.2 The Director may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:

38.2.1 any Central Government Body; or

38.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Director,

and the Supplier shall, at the Director's request, enter into a novation agreement in such form as the Director shall reasonably specify in order to enable the Director to exercise its rights pursuant to this Clause 38.2.

38.3 A change in the legal status of the Director such that it ceases to be a Central Government Body shall not (subject to Clause 38.4) affect the validity of this Agreement and this Agreement shall be binding on any Successor Body to the Director.

38.4 If the Director assigns, novates or otherwise disposes of any of its rights, obligations or liabilities under this Agreement to a body which is not a Central Government Body or if a body which is not a Central Government Body succeeds the Director (any such body a "**Successor Body**"), the Supplier shall have the right to terminate for an Insolvency Event affecting the Successor Body identical to the right of termination of the Director under limb (k) of the definition of Supplier Termination Event (as if references in that limb (k) to the Supplier and the Guarantor were references to the Successor Body).

39 WAIVER AND CUMULATIVE REMEDIES

39.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by Law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

39.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by Law, in equity or otherwise.

40 RELATIONSHIP OF THE PARTIES

40.1 Except as expressly provided otherwise in this Agreement, nothing in this Agreement, nor any actions taken by the Parties pursuant to this Agreement, shall create a partnership, joint venture or relationship of employer and employee or principal and agent between the Parties, or authorise either Party to make representations or enter into any commitments for or on behalf of any other Party.

41 PREVENTION OF FRAUD AND BRIBERY

41.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Supplier Personnel, have at any time prior to the Effective Date:

41.1.1 committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or

41.1.2 been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

41.2 The Supplier shall not during the term of this Agreement:

41.2.1 commit a Prohibited Act; and/or

41.2.2 do or suffer anything to be done which would cause the Director or any of the Director's employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

41.3 The Supplier shall during the term of this Agreement:

41.3.1 establish, maintain and enforce, and require that its Sub-contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

41.3.2 have in place reasonable prevention measures (as defined in sections 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

41.3.3 keep appropriate records of its compliance with its obligations under Clause 41.3.1 and make such records available to the Director on request; and

41.3.4 take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with Section 47 of the Criminal Finances Act 2017.

41.4 The Supplier shall immediately notify the Director in writing if it becomes aware of any breach of Clause 41.1 and/or 41.2, or has reason to believe that it has or any of the Supplier Personnel have:

41.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

41.4.2 been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

41.4.3 received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Agreement or otherwise suspects that any person or Party directly or indirectly connected with this Agreement has committed or attempted to commit a Prohibited Act.

41.5 If the Supplier makes a notification to the Director pursuant to Clause 41.4, the Supplier shall respond promptly to the Director's enquiries, co-operate with any investigation, and allow the Director to Audit any books, Records and/or any other relevant documentation in accordance with Clause 12 (*Records, Reports, Audits & Open Book Data*).

41.6 If the Supplier is in Default under Clauses 41.1 and/or 41.2, the Director may by notice:

41.6.1 require the Supplier to remove from performance of this Agreement any Supplier Personnel whose acts or omissions have caused the Default; or

41.6.2 immediately terminate this Agreement.

41.7 Any notice served by the Director under Clause 41.6 shall specify the nature of the Prohibited Act, the identity of the Party who the Director believes has committed the Prohibited Act and the action that the Director has elected to take (including, where relevant, the date on which this Agreement shall terminate).

42 CONFLICTS OF INTEREST

42.1 The Supplier undertakes at all times during the Term to avoid creating a conflict of interest as provided for in this Clause 42 (*Conflicts of Interest*). For these purposes, the Supplier acknowledges and agrees that a conflict of interest shall arise where:

42.1.1 in its provision of the Services, the Supplier is required to advise upon or select the provision of any goods or services (including software) from any third party; and

42.1.2 the Supplier's advice or selection is either made as a consequence of its consideration of, or is materially influenced by, factors other than the Director's best interests; or

42.1.3 in the circumstances set out in Clause 42.2, the Supplier fails to adhere to the procedures described in that Clause;

(each a "**Conflict of Interest**").

42.2 If the Supplier wishes to submit a tender to the Director in relation to any re-tender of the Services or tender for new services, the Supplier shall if requested, demonstrate to the Director's or Service Recipients' reasonable satisfaction and otherwise ensure at all material times that:

42.2.1 such tender is not made with the benefit of any of the Director Confidential Information;

42.2.2 unless otherwise agreed in writing by the Director or Service Recipients, those Supplier Personnel who are providing the Services and who receive the Director Confidential Information (the **"Business as Usual Team"**) are not involved (and have not been involved) in the tender process in any way and do not directly or indirectly discuss with, or provide such information to, persons involved in the tender during the tender process (the **"Bid Team"**);

42.2.3 any Director Confidential Information is not available to the Bid Team and that such Director Confidential Information is stored on separate computer systems or segregated areas of the Supplier's computer systems which cannot be accessed by any member of the Bid Team;

42.2.4 the Bid Team and the Business as Usual Team have an appropriate level of physical separation and are, so far as practicable, located in different offices, or different floors of the same offices, of the Supplier; and

42.2.5 the Bid Team and the Business as Usual Team have, so far as is reasonable, separate reporting and management lines unless otherwise agreed in writing by the Director or Service Recipient.

42.3 The Supplier shall make any selection or acquisition of any goods or services for the Director pursuant to this Agreement and give advice relating to such selection or acquisition in the best interests of the Director, irrespective of (whether arising directly or indirectly from such selection or acquisition) any interests of and potential benefits for the Supplier, the Sub-contractors and all members of the Supplier Group and all Sub-contractor Groups. For the purposes of this Clause 42, 'benefit' shall include in respect of any such goods or services the receipt of either any consideration or any other benefit which is not passed on to the Director.

42.4 If the Supplier becomes aware of any Conflict of Interest (whether such existed before the Effective Date or afterwards) it shall immediately notify the Director of the Conflict of Interest and provide full details of the Conflict of Interest together with any additional information which the Director may require in connection with such matter.

42.5 If the Director reasonably considers that the Conflict of Interest notified to the Director under Clause 42.4 is capable of being avoided or removed, the Director may require the Supplier to take such steps as are necessary to avoid or, as the case may be, remove such Conflict of Interest in accordance with the provisions in Clause 29 (*Rectification Plan Process*).

42.6 If:

42.6.1 the Supplier fails to remedy such Conflict of Interest as required in Clause 42.5; or

42.6.2 such Conflict of Interest cannot be remedied; or

42.6.3 the Director considers that a Conflict of Interest existed at the Effective Date,

such matter shall be deemed to constitute a material Default.

43 SEVERANCE

43.1 If any provision of this Agreement (or part of any provision) is held to be void or otherwise unenforceable by any court of competent jurisdiction, such provision (or part) shall to the extent necessary to ensure that the remaining provisions of this Agreement are not void or unenforceable be deemed to be deleted and the validity and/or enforceability of the remaining provisions of this Agreement shall not be affected.

43.2 In the event that any deemed deletion under Clause 43.1 is so fundamental as to prevent the accomplishment of the purpose of this Agreement or materially alters the balance of risks and rewards in this Agreement, either Party may give notice to the other Party requiring the Parties to commence good faith negotiations to amend this Agreement so that, as amended, it is valid and enforceable, preserves the balance of risks and rewards in this Agreement and, to the extent that is reasonably possible, achieves the Parties' original commercial intention.

43.3 If the Parties are unable to agree on the revisions to this Agreement within five (5) Working Days of the date of the notice given pursuant to Clause 43.2, the matter shall be dealt with in accordance with Paragraph 4 (*Negotiation*) of Schedule 8.3 (*Dispute Resolution Procedure*) except that if the representatives are unable to resolve the dispute within thirty (30) Working Days of the matter being referred to them, this Agreement shall automatically terminate with immediate effect. The costs of termination incurred by the Parties shall lie where they fall if this Agreement is terminated pursuant to this Clause 43.3.

44 FURTHER ASSURANCES

44.1 Each Party undertakes at the request of the other, and at the cost of the requesting Party to do all acts and execute all documents which may be reasonably necessary to give effect to the meaning of this Agreement.

45 ENTIRE AGREEMENT

45.1 This Agreement constitutes the entire agreement between the Parties in respect of its subject matter and supersedes and extinguishes all prior negotiations, arrangements, understanding, course of dealings or agreements made between the Parties in relation to its subject matter, whether written or oral.

45.2 Neither Party has been given, nor entered into this Agreement in reliance on, any warranty, statement, promise or representation other than those expressly set out in this Agreement.

45.3 Nothing in this Clause 45 shall exclude any liability in respect of misrepresentations made fraudulently.

46 THIRD PARTY RIGHTS

46.1 The provisions of Clause 20.1 (*IPRs Indemnity*), Paragraphs 2.1 and 2.6 of Part 1, Paragraphs 2.1, 2.6, 3.1 and 3.3 of Part 2, Part 4 and Paragraphs 1.4, 2.3 and 2.8 of Part 5 of Schedule 9.1 (*Staff Transfer*) and the provisions of Paragraph 6.9 of Schedule 8.5 (*Exit Management*) (together "**Third Party Provisions**") confer benefits on persons named or identified in such provisions other than the Parties (each such person a "**Third Party Beneficiary**") and are intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

46.2 Subject to Clause 46.1, a person who is not a Party to this Agreement has no right under the CRTPA to enforce any term of this Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

46.3 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Director, which may, if given, be given on and subject to such terms as the Director may determine.

46.4 Any amendments or modifications to this Agreement may be made, and any rights created under Clause 46.1 may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

47 NOTICES

47.1 Any notices sent under this Agreement must be in writing.

47.2 Subject to Clause 47.4, the following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending.	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next Working Day service providing proof of delivery	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed, prepaid and delivered as evidenced by signature of a delivery receipt

47.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

	Supplier	Director
Contact	For the attention of: Legal Director Copied to: Commercial Director, Private Sector	For the attention of: Head of Supply Chain and Procurement
Address	Sopra Steria	NS&I

	Three Cherry Trees Lane Hemel Hempstead Hertfordshire HP2 7AH	Sanctuary Buildings Great Smith Street London SW1P 3BT
Email	[redacted] Copied to: [redacted]	[redacted]

47.4 The following notices may only be served as an attachment to an email if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in the table in Clause 47.2:

47.4.1 Step-In Notices;

47.4.2 Force Majeure Notices;

47.4.3 notices issued by the Supplier pursuant to Clause 35.3 (*Termination by the Supplier*);

47.4.4 Termination Notices; and

47.4.5 Dispute Notices.

47.5 Failure to send any original notice by personal delivery or recorded delivery in accordance with Clause 47.4 shall invalidate the service of the related e-mail transmission. The deemed time of delivery of such notice shall be the deemed time of delivery of the original notice sent by personal delivery or Royal Mail Signed For™ 1st Class delivery (as set out in the table in Clause 47.2) or, if earlier, the time of response or acknowledgement by the other Party to the email attaching the notice.

47.6 This Clause 47 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any adjudication or other method of dispute resolution (other than the service of a Dispute Notice under Schedule 8.3 (*Dispute Resolution Procedure*)).

48 DISPUTES

48.1 The Parties shall resolve Disputes arising out of or in connection with this Agreement in accordance with the Dispute Resolution Procedure.

48.2 The Supplier shall continue to provide the Services in accordance with the terms of this Agreement until a Dispute has been resolved.

49 GOVERNING LAW AND JURISDICTION

49.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

49.2 Subject to Clause 48 (*Disputes*) and Schedule 8.3 (*Dispute Resolution Procedure*) (including the Director's right to refer the dispute to arbitration), the Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

This Agreement has been duly executed by the Parties on the date which appears at the head of its first page.

SIGNED for and on behalf of **SOPRA STERIA** by a director:	)	
	)	Signature:
		Name (block capitals):
		Director
SIGNED for and on behalf of the **DIRECTOR OF SAVINGS**	)	
	)	Signature:
		Name (block capitals):
		Position:

SCHEDULE 1 - DEFINITIONS

1 Definitions

1.1 Unless otherwise provided or the context otherwise requires the following expressions shall have the meanings set out below.

Access Permission means access rights for users to access and use the Virtual Library.

Accounting Reference Date means in each year the date to which the Supplier prepares its annual audited financial statements.

Achieve means:

(a) in respect of a Test, to successfully pass a Test without any Test Issues; and

(b) in respect of a Milestone, the issue of a Milestone Achievement Certificate in respect of that Milestone in accordance with the provisions of Schedule 6.2 (*Testing Procedures*),

and "**Achieved**" and "**Achievement**" shall be construed accordingly.

Acquired Rights Directive means the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time.

Actionable Insight means interrogating and applying critical thought to empirical data in order to evaluate service performance and recommend ways to improve Customer and operation outcomes, which may include, but is not limited to, provision and analysis of data collected across the Services provided by the Supplier or Relevant Third Party Suppliers on service performance, Customer behaviours and Customer impacts, journey analytics, attitudinal research and survey data.

Additional Services means the those services within the scope of the Find a Tender Notice which includes but is not limited to the services described as Additional Services in Schedule 2.1 (*Services Description*), the on boarding of Relevant Third Party Suppliers and any B2B Services (as applicable), which are to be provided by the Supplier if required by the Director, in accordance with Clause 5.11 (*Additional Services*).

Affected Party means 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.

Agent means any personnel who has voice or digital contact with a Customer.

Agreement means the main body terms and conditions of this Agreement together with all Schedules appended to it, and the Collaboration Agreement.

Allowable Assumptions means the assumptions referred to in Paragraph 7 of Part 3 of Schedule 7.1 (*Charges and Invoicing*) and as detailed in the Pricing Response Template.

Annual Contract Report has the meaning given in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Annual Revenue means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:

(a) figures for accounting periods of other than twelve (12) months should be scaled pro rata to produce a proforma figure for a twelve (12) month period; and

(b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date.

Anticipated Contract Life Profit Margin has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

API Enablement Project (or **AEP**) means the Director's project(s) with the Incumbent Supplier to deliver the APIs to bridge the to be agreed functionality gap between the Incumbent Supplier estate and what is needed to support the relevant delivery of Services under this Agreement which is currently in design and where the scope is due to be initiated by the Director.

Approved Sub-Licensee means any of the following:

(a) a Central Government Body;

(b) any third party providing services to a Central Government Body; and/or

(c) any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Director.

Assets means all assets and rights used by the Supplier to provide the Services in accordance with this Agreement but excluding the Director Assets.

Assisted Digital means the provision of support to Customers unable to self-serve digitally, to guide them through their Digital Self-Service journey or operate it on their behalf.

Associated Person has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017.

Associates means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of Control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles.

Assurance means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority.

Audit means any exercise by the Director of its Audit Rights pursuant to Clause 12 (*Records, Reports, Audits & Open Book Data*) and Schedule 7.5 (*Financial Reports, Audit and Risk*).

Audit Agents means:

(a) the Director's statutory or regulatory auditors;

(b) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;

(c) HM Treasury or the Cabinet Office;

(d) any party formally appointed by the Director to carry out audit or similar review functions;

(e) as defined in Schedule 7.5 (*Financial Reports, Audit and Risk);*

(f) the Director's internal and external auditors; and

(g) successors or assigns of any of the above.

Audit Rights means the audit and access rights referred to in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Authenticated Retail Website means the Customer-facing website, enabling Digital Self-Service for Authenticated Customers (also known as the transactional website).

Authentication means the process of gaining access to computer systems by reasserting an established trust relationship through the exchange of previously-created Authentication Credentials and "**Authenticate**" and "**Authenticated**" shall be construed accordingly.

Authentication Credentials means a Customer's, or User's (as appropriate), Authentication information used to reassert an established trust relationship. Typically consists of a Customer, or User (as appropriate), identifier and multiple factors from knowledge, possession and inherence.

Authority to Proceed (or **ATP**) means the authorisation to the Supplier to commence the provision of the relevant Operational Services to the Director, provided by the Director in the form of a Milestone Achievement Certificate in respect of the ATP Milestone.

B2B Service means any business to business service which the Director operates on behalf of a third party customer through the Services (as applicable), which may include services provided to other government departments through NS&I Government Payment Services (NS&I GPS), which extend the Services to further Service Recipients for the purposes of increasing the utilisation of the assets and exploiting the capacity, capability and know-how used to deliver the Services, subject to the limitations set out in the Find a Tender Notice.

Baseline Security Requirements means the Director's baseline security requirements, the current copy of which is contained in Annex 1 of Schedule 2.4 (*Security Management*), as updated from time to time by the Director and notified to the Supplier.

Board means the Supplier's board of directors.

Board Confirmation means the written confirmation from the Board in accordance with Paragraph 8 of Schedule 7.4 (*Financial Distress*).

Breakage Costs Payment has the meaning given in Schedule 7.2 (*Payments on Termination*).

Cabinet Office Markets and Suppliers Team means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function.

Central Government Body or Government means 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 for National Statistics:

(a) Government Department;

(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);

(c) Non-Ministerial Department; or

(d) Executive Agency.

Certificate of Costs has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

Change means any change to this Agreement, the Collaboration Agreement or such other change which is the subject to Schedule 8.2 (*Change Control Procedure*) as the context requires.

Change Authorisation Note means a form setting out an agreed Contract Change which shall be substantially in the form of Annex 3 of Schedule 8.2 (*Change Control Procedure*).

Change Control Procedure means the procedure for changing this Agreement set out in Schedule 8.2 (*Change Control Procedure*).

Change in Law means any change in Law which impacts on the performance of the Services which comes into force after the Effective Date.

Change Proposal has the meaning given in Schedule 8.2 (*Change Control Procedure*).

Change Request means a written request for a Contract Change substantially in the form of Annex 2 of Schedule 8.2 (*Change Control Procedure*).

Channel means the medium of interaction between the Customer and the Director, through which Touchpoints are delivered.

Charges means the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 7.1 (*Charges and Invoicing*), including any Milestone Payment or Service Charge.

Class 1 Transaction has the meaning set out in the listing rules issued by the UK Listing Director.

CNI means Critical National Infrastructure.

Collaboration Agreement means the form of collaboration agreement set out in Schedule 12 or the Supplier-executed version.

Commercially Sensitive Information means the information listed in Schedule 4.2 (*Commercially Sensitive Information*) comprising the information of a commercially sensitive nature relating to:

(a) the pricing of the Services;

(b) details of the Supplier's IPRs; and

(c) the Supplier's business and investment plans;

which the Supplier has indicated to the Director that, if disclosed by the Director, would cause the Supplier significant commercial disadvantage or material financial loss.

Comparable Supply means the supply of services to other customers of the Supplier that are the same or similar to any of the Services including both other government customers and non-government customers working in the financial services industry.

Compensation for Unacceptable KPI Failure has the meaning given in Clause 7.3.1 (*Unacceptable KPI Failure*).

Compensation and Goodwill Payment means a payment made to a Customer following receipt of a complaint, in accordance with the Director's Compensation and Goodwill Policy and following the procedure set out in Part 3, Paragraph 4 of Schedule 7.1 (*Charges and Invoicing*).

Compensation and Goodwill Payments Report has the meaning given in Part 3, Paragraph 4.3 of Schedule 7.1 *(Charges and Invoicing).*

Compensation Credits means credits payable by the Supplier or any Relevant Third Party Supplier to the Director as a result of any Compensation and Goodwill Payments being attributed to that Relevant Third Party Supplier by the Supplier in a Service Period, calculated in accordance with Part 3, Paragraph 4.5 of Schedule 7.1 (*Charges and Invoicing*).

Compensation Payment has the meaning given in Schedule 7.2 (*Payments on Termination*).

Condition Precedent has the meaning given in Clause 4.2 (*Condition Precedent*).

Confidential Information means:

(a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Agreement that relates to:

(i) the Disclosing Party Group; or

(ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group;

(b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Agreement that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Agreement;

(c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Agreement and all matters arising therefrom; and

(d) Information derived from any of the above,

but not including any Information which:

(i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;

(ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;

(iii) obtained otherwise than by a breach of this Agreement or breach of a duty of confidentiality;

(iv) was independently developed without access to the Confidential Information; or

(v) relates to the Supplier's:

(1) performance under this Agreement; or

(2) failure to pay any Sub-contractor as required pursuant to Clause 15.16 (*Supply Chain Protection*).

Conflict of Interest has the meaning given in Clause 42.1 (*Conflicts of Interest*).

Contact Centre means the contact centre where Customers interact with Agents including chat, voice calls, messaging, e-mail and other forms of direct communication.

Continuous Improvement Plan means the plan produced and maintained by the Director in conjunction with the Supplier and Relevant Third Party Suppliers, as described in Schedule 8.8 (*Continuous Improvement*).

Contract Change means any change to this Agreement other than an Operational Change.

Contract Inception Report means the initial financial model in the form of the Pricing Response Template, as agreed by the Supplier and the Director in writing on or before the Effective Date.

Contracts Finder means the online government portal which allows suppliers to search for information about contracts worth over £10,000 (ten thousand pounds) (excluding VAT) as prescribed by Part 4 of the Public Contract Regulations 2015.

Contract Year means:

(a) a period of twelve (12) months commencing on the Effective Date; or

(b) thereafter a period of twelve (12) months commencing on each anniversary of the Effective Date;

provided that the final Contract Year shall end on the expiry or termination of the Term.

Control means the possession by person, directly or indirectly, of 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.

Controller has the meaning given in the UK GDPR.

Corporate Change Event means:

(a) any change of Control of the Supplier or a Parent Undertaking of the Supplier;

(b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Director, could have a material adverse effect on the Services;

(c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Director, could have a material adverse effect on the Services;

(d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;

(e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;

(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding twenty five percent (25%) of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any twelve (12) month period;

(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;

(h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;

(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or

(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales.

Corporate Resolution Planning Information means, together, the:

(a) Group Structure Information and Resolution Commentary; and

(b) UK Public Sector and CNI Contract Information.

Costs has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

CPP Milestone means a contract performance point as set out in the Implementation Plan, being the Milestone at which the Supplier has demonstrated that the Supplier Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 6.2 (*Testing Procedures*).

Critical National Infrastructure means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

(a) major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

(b) significant impact on the national security, national defence, or the functioning of the UK.

Critical Performance Failure means:

(a) the Supplier accruing in aggregate two hundred and fifty five (255) or more Service Points (in terms of the number of points allocated) in any period of three (3) months; or

(b) the Supplier accruing Service Credits or Compensation for Unacceptable KPI Failure which meet or exceed the Service Credit Cap.

Critical Service Contract means the overall status of the Services provided under this Agreement as determined by the Director and specified in Paragraph 1.1 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

CRP Information means the Corporate Resolution Planning Information.

CRTPA means the Contracts (Rights of Third Parties) Act 1999.

Customer means an individual or organisation who is either:

(a) an existing, prospective or past holder of a Product; or

(b) a third party acting on behalf of a Customer (for example a “Responsible Person” as defined in the Product Terms and Conditions, a financial advisor, solicitor or executor); or

(c) an existing, prospective or past Service Recipient.

Customer Due Diligence means the gathering of information relevant to a Customer's affairs, which in turn allows an assessment of the extent of potential risks, having regard to the Joint Money Steering Group (JMLSG) guidance and ensuring compliance with the Money Laundering Regulations.

Data Loss Event means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Protection Impact Assessment means a process to help the Controller identify and minimise the risks of the envisaged processing on the protection of Personal Data.

Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the DPA 2018; the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and the guidance and codes of practice issued by the Information Commissioner and which are applicable to a Party.

Data Protection Officer has the meaning given in the UK GDPR.

Data Subject has the meaning given in the DPA.

Data Subject Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data.

Deductions means all Service Credits, Compensation for Unacceptable KPI Failure or any other deduction which is paid or payable to the Director under this Agreement.

Default means any breach of the obligations of the relevant Party (including failure to meet obligations under the Collaboration Agreement or abandonment of this Agreement in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement:

(a) in the case of the Director, of its employees, servants, agents; or

(b) in the case of the Supplier, of its Sub-contractors or any Supplier Personnel,

in connection with or in relation to the subject-matter of this Agreement (including the Collaboration Agreement) and in respect of which such Party is liable to the other.

Defect means:

(a) any error, damage or defect in the manufacturing of a Deliverable; or

(b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or

(c) any failure of any Deliverable to provide the performance, features and functionality specified in the Director Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria; or

(d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Director Requirements or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from meeting its associated Test Success Criteria.

Definition Phase has the meaning given in Schedule 8.2 (*Change Control Procedure*).

Delay means:

(a) a delay in the Achievement of a Milestone by its Milestone Date; or

(b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan.

Deliverable means an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Agreement.

Dependencies has the meaning given in the Collaboration Agreement.

Dependent Parent Undertaking means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Agreement, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Agreement.

Detailed Implementation Plan means the plan developed and revised from time to time in accordance with Paragraphs 4 and 5 of Schedule 6.1 (*Implementation Plan*).

Development Pool: means a pre-defined group of Supplier resources (as set out in Table 49 of Schedule 4.1 (*Supplier Solution*) or as otherwise agreed in accordance with Paragraph 4 of Schedule 8.2 (*Change Control Procedure*) that are available to provide DevOps Change and some other changes that will support the Continuous Improvement Plan as described in Schedule 8.8 (*Continuous Improvement*).

DevOps means a function that combines development and operational activities in a single working group.

Digital Channel means Channels where Customers interact directly with the Director using digital devices, including the Mobile Channel, the Internet Channel, voice assistants, chat and chatbots, social media and Digital Communications Channels.

Digital Communications Channels means Channels which enable digital communications between the Director and Customers, including SMS, push notifications, messaging, email and Secure Messages.

Digital Self-Service means Customers self-serving end-to-end via Digital Touchpoints, with no unwanted deflection to post or phone, even for exceptions, underpinned by straight-through automated processes with no human interaction or workarounds.

Digital Touchpoint means the combination of Digital Self-Service and Digital Channel.

Director Assets means the Director Materials, the Director infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Director and which is or may be used in connection with the provision or receipt of the Services.

Director Background IPRs means:

(a) IPRs owned by the Director before the Effective Date, including IPRs contained in any of the Director's Know-How, documentation, processes and procedures;

(b) IPRs created by the Director independently of this Agreement; and/or

(c) Crown Copyright which is not available to the Supplier otherwise than under this Agreement;

but excluding IPRs owned by the Director subsisting in the Director Software and the Trade Marks.

Director Cause means any material breach by the Director of any of the Director Responsibilities, except to the extent that such breach is:

(a) the result of any act or omission by the Director to which the Supplier has given its prior consent; or

(b) caused by the Supplier, any Sub-contractor or any Supplier Personnel.

Director Data means:

(a) 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:

(i) supplied to the Supplier by or on behalf of the Director; and/or

(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or

(b) any Personal Data for which the Director is the Data Controller.

Director IT Strategy means the Director's IT policy in force as at the Effective Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Change Control Procedure.

Director Materials means the Director Data together with any materials, documentation, information, programs and codes supplied by the Director to the Supplier, the IPRs in which:

(a) are owned or used by or on behalf of the Director; and

(b) are or may be used in connection with the provision or receipt of the Services,

but excluding any Project Specific IPRs, Specially Written Software, Supplier Software, Third Party Software and Documentation relating to Supplier Software or Third Party Software.

Director Premises means premises owned, controlled or occupied by the Director and/or any Central Government Body which are made available for use by the Supplier or its Sub-contractors for provision of the Services (or any of them).

Director Representative means the representative appointed by the Director pursuant to Clause 11.4 (*Representatives*).

Director Requirements means the requirements of the Director set out in Schedule 2.1 (*Services Description*), Schedule 2.2 (*Performance Levels*), Schedule 2.3 (*Standards*), Schedule 2.4 (*Security Management*), Schedule 2.5 (*Insurance Requirements*), Schedule 6.1 (*Implementation Plan*), Schedule 7.6 (*Regulatory Compliance and Financial Crime*), Schedule 8.4 (*Reports and Records Provisions*), Schedule 8.5 (*Exit Management*) and Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

Director Responsibilities means the responsibilities of the Director specified in Schedule 3 (*Director Responsibilities*).

Director Software means software which is owned by or licensed to the Director (other than under or pursuant to this Agreement) and which is or will be used by the Supplier for the purposes of providing the Services.

Director System means the Director's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Director or the Supplier in connection

with this Agreement which is owned by the Director or licensed to it by a third party and which interfaces with the Supplier System or which is necessary for the Director to receive the Services.

Disclosing Party has the meaning given in Clause 23.1 *(Confidentiality).*

Disclosing Party Group means:

(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and

(b) where the Disclosing Party is the Director, the Director and any Central Government Body with which the Director or the Supplier interacts in connection with this Agreement.

Dispute means 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 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, save where in relation to the allocation of Compensation and Goodwill Payments (which shall be dealt with in accordance with the provisions of Part 3, Paragraph 4 of Schedule 7.1 (*Charges and Invoicing*)).

Dispute Notice has the meaning given in Paragraph 2.1 of Schedule 8.3 (*Dispute Resolution Procedure*).

Dispute Resolution Procedure means the dispute resolution procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*).

Documentation means descriptions of the Services and Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf components and (ii) Source Code and build information for proprietary components), relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as:

(a) is required to be supplied by the Supplier to the Director under this Agreement;

(b) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Director to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide Services;

(c) is required by the Supplier in order to provide the Services; and/or

(d) has been or shall be generated for the purpose of providing the Services.

DOTAS means the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC 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 section 132A of the Social Security Administration Act 1992.

DPA means the Data Protection Act 2018.

Due Diligence Information means any information supplied to the Supplier by or on behalf of the Director prior to the Effective Date.

Effective Date means the later of:

(a) the date on which this Agreement is signed by both Parties;

(b) the date on which the Condition Precedent has been satisfied or waived in accordance with Clause 4.2 (*Condition Precedent*); and

(c) the Implementation Services Commencement Date.

EIRs means the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations.

Emergency Maintenance means ad hoc and unplanned maintenance provided by the Supplier where:

(a) the Director reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may have developed a fault, and notifies the Supplier of the same; or

(b) the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault.

Employee Liabilities means all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation related to employment including in relation to the following:

(a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;

(b) unfair, wrongful or constructive dismissal compensation;

(c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;

(d) compensation for less favourable treatment of part-time workers or fixed term employees;

(e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions;

(f) employment claims whether in tort, contract or statute or otherwise; and/or

(g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation.

Employment Regulations means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the Acquired Rights Directive.

End to End Service means the Services and the Related Services delivering an end to end solution to the Director by the Supplier and any Relevant Third Party Supplier.

Estimated Year 1 Charges means the estimated Charges payable by the Director during the first Contract Year, as set out in the Financial Model.

Estimated Initial Service Charges means the estimated Service Charges payable by the Director during the period of twelve (12) months from the first Operational Service Commencement Date, as set out in the Financial Model.

Euro Compliant means that: (i) the introduction of the euro within any part(s) of the UK shall not affect the performance or functionality of any relevant items nor cause such items to malfunction, end abruptly, provide invalid results or adversely affect the Director's business; (ii) all currency-reliant and currency-related functions (including all calculations concerning financial data) of any relevant items enable the introduction and operation of the euro; and (iii) in particular each and every relevant item shall, to the extent it performs or relies upon currency-related functions (including all calculations concerning financial data):

(a) be able to perform all such functions in any number of currencies and/or in euros;

(b) during any transition phase applicable to the relevant part(s) of the UK, be able to deal with multiple currencies and, in relation to the euro and the national currency of the relevant part(s) of the UK, dual denominations;

(c) recognise accept, display and print all the euro currency symbols and alphanumeric codes which may be adopted by any government and other European Union body in relation to the euro;

(d) incorporate protocols for dealing with rounding and currency conversion;

(e) recognise data irrespective of the currency in which it is expressed (which includes the euro) and express any output data in the national currency of the relevant part(s) of the UK and/or the euro; and

(f) permit the input of data in euro and display an outcome in euro where such data, supporting the Director's normal business practices, operates in euro and/or the national currency of the relevant part(s) of the UK.

Executive Committee has the meaning given in Schedule 8.1 (*Governance*).

Exit Day shall have the meaning in the European Union (Withdrawal) Act 2018.

Exit Management means services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Director and/or a Replacement Supplier, as set out or referred to in Schedule 8.5 (*Exit Management*).

Exit Plan means the plan produced and updated by the Supplier during the Term in accordance with Paragraph 4 of Schedule 8.5 (*Exit Management*).

Expedited Dispute Timetable means the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 8.3 (*Dispute Resolution Procedure*).

Expert has the meaning given in Schedule 8.3 (*Dispute Resolution Procedure*).

Expert Determination means the process described in Paragraph 6 of Schedule 8.3 (*Dispute Resolution Procedure*).

Extension Period means a period of one (1) year from the end of the Initial Term.

Fair Deal has the meaning given in Schedule 9.1 (*Staff Transfer*).

Financial Distress Event means the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 7.4 (*Financial Distress*).

Financial Distress Remediation Plan means a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Agreement in the event that a Financial Distress Event occurs.

Financial Model has the meaning given in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Financial Reports has the meaning given in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Financial Transparency Objectives has the meaning given in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Find a Tender Notice means the notice issued by the Director on 29th April 2022 on the Find a Tender Service with reference number 2022/S 000-011240 .

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

Force Majeure Event means any event outside the reasonable control of either Party affecting its performance of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier's or a Sub-contractor's supply chain.

Force Majeure Notice means a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event.

Former Supplier has the meaning given in Schedule 9.1 (*Staff Transfer*).

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 to avoid national insurance contributions.

General Change in Law means a Change in Law where the change is of a general legislative nature including:

(a) taxation or duties of any sort affecting the Supplier or the Services;

(b) any Law relating generally to government or financial services, including private sector financial services;

(c) any changes to the laws, regulations and guidance identified in Schedule 7.6 (*Regulatory Compliance and Financial Crime*); or

(d) one which affects or relates to a Comparable Supply.

Good Industry Practice means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services or part of them (as appropriate to the context in which this expression is used) similar to or the same as the Services to a customer like the Director, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws.

Group Structure Information and Resolution Commentary means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Annex 1 of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

Guarantee means the deed of guarantee in favour of the Director entered into by the Guarantor on or about the date of this Agreement (which is in the form set out in Schedule 10 (*Guarantee*)), or any guarantee acceptable to the Director that replaces it from time to time.

Guarantor means **SOPRA STERIA SA**, a company incorporated in **France** with registered number **326 820 065** and whose registered office is at **PAE Les Glaisins, Annecy-le-Vieux, 74940 Annecy**.

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

Health and Safety Policy means the health and safety policy of the Director and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety.

HMRC means HM Revenue & Customs.

Impact Assessment has the meaning given in Schedule 8.2 (*Change Control Procedure*).

Implementation Plan means the Outline Implementation Plan or the Detailed Implementation Plan pursuant to Schedule 6.1 (*Implementation Plan*) as updated in accordance with Paragraph 5 of Schedule 6.1 (*Implementation Plan*) from time to time.

Implementation Services means the implementation services described as such in the Services Description.

Implementation Services Commencement Date means the date on which the Supplier is to commence provision of the first of the Services, as set out in Schedule 6.1 (*Implementation Plan*).

Incumbent Supplier means Atos IT Services UK Limited (a company registered in England with registration number 01245534) which manages sales processing and customer services, in addition to IT and infrastructure services under the Legacy Services Contract.

Indemnified Person means the Director and each and every person to whom the Director (or any direct or indirect sub-licensee of the Director) sub-licenses, assigns or novates any Relevant IPRs or rights in Relevant IPRs in accordance with this Agreement.

Independent Control means where a Controller has provided Personal Data to another Party which is neither a Processor or Joint Controller because the recipient itself determines the purposes and means of processing but does so separately from the Controller providing it with Personal Data.

Information means all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form).

Initial Term means the period of five (5) years from the 1st April 2024.

Initial Upload Date means the occurrence of an event detailed in Schedule 8.4 (*Reports and Records Provisions*), Annex 3 (*Virtual Library*) which requires the Supplier to provide its initial upload of the relevant information to the Virtual Library.

Insolvency Event with respect to any person, means:

(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:

(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or

(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;

(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;

(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;

(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

(f) where that person is a company, a LLP or a partnership:

(i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at court or given or if an administrator is appointed, over that person;

(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or

(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above.

Insurances has the meaning given in Schedule 2.5 (*Insurance Requirements*).

Intellectual Property Rights (or **IPRs**) means:

(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.

Internet Channel means the retail internet Channel comprising of the Public Retail Website and the Authenticated Retail Website, and their supporting systems and services.

Intervention Cause has the meaning given in Clause 31.1 (*Remedial Adviser*).

Intervention Notice has the meaning given in Clause 31.1 (*Remedial Adviser*).

Intervention Period has the meaning given in Clause 31.2.4 (*Remedial Adviser*).

Intervention Trigger Event means:

(a) any event falling within limb (a), (b), (c), (e), (f) or (g) of the definition of a Supplier Termination Event;

(b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services;

(c) the Supplier accruing in aggregate:

(i) sixty (60) or more Service Points (in terms of the number of points allocated) in respect of any one Key Performance Indicator in any period of two (2) months; or

(ii) one hundred (100) or more Service Points (in terms of the number of points allocated) in respect of any or all Key Performance Indicators any period of three (3) months;

(d) the Supplier accruing Service Credits which meet or exceed seventy-five percent (75%) of the Service Credit Cap;

(e) the Supplier not Achieving a Key Milestone within seventy-five (75) days of its relevant Milestone Date; and/or

(f) a Default by the Supplier under the Collaboration Agreement that materially prevents or delays the performance of any of the services or obligations of a Relevant Third Party Supplier.

IPRs Claim means any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, or the use of the Director Software by or on behalf of the Supplier, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Agreement or for a purpose not reasonably to be inferred from the Services Description or the provisions of this Agreement.

IT means information and communications technology.

IT Environment means the Director System and the Supplier System.

ISFT means invitation to submit final tender.

Joint Controllers means where two or more Controllers jointly determine the purposes and means of processing.

Key Milestone means the Milestones identified in the Implementation Plan as key milestones.

Key Performance Indicator means the key performance indicators set out in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Key Personnel means those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in Schedule 9.2 (*Key Personnel*) against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (*Key Personnel*).

Key Roles means a role described as a Key Role in Schedule 9.2 (*Key Personnel*) and any additional roles added from time to time in accordance with Clause 14.4 (*Key Personnel*).

Key Sub-contract means each Sub-contract with a Key Sub-contractor.

Key Sub-contractor means any Sub-contractor:

(a) which, in the opinion of the Director, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or

(b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten percent (10%) of the aggregate Charges forecast to be payable under this Agreement (as set out in the Financial Model).

Know-How means all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party's possession before this Agreement.

Knowledge and Insight Function means the Director's central function collating and analysing data and Actionable Insight from across the End to End Service to generate insights, providing the Director with greater knowledge of its Customers, enabling better Customer service and an improved experience for the Customer.

KPI Failure means a failure to meet the Target Performance Level in respect of a Key Performance Indicator.

KPI Service Threshold shall be as set out against the relevant Key Performance Indicator in Table 1 of Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Law means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier or the Director is bound to comply or which the Director has decided voluntarily to comply, including but not limited to those identified in Schedule 7.6 (*Regulatory Compliance and Financial Crime*).

LED means Law Enforcement Directive *(Directive (EU) 2016/680)*.

Legacy Services Contract means the agreement for Business Processing Services between the Incumbent Supplier and the Director dated 20th May 2013 (and restated July 2019).

Licensed Software means all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Director for the purposes of or pursuant to this Agreement, including any Supplier Software, Third Party Software and/or any Specially Written Software.

Long Stop Date means the latest date(s) by which the Operational Services must be fully available and functional as set out in Schedule 6.1 (*Implementation Plan*).

Losses means losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise.

Maintenance Schedule shall have the meaning set out in Clause 9.4 (*Maintenance*).

Malicious Software means 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 means the management information specified in Schedule 2.2 (*Performance Levels*), Schedule 7.1 (*Charges and Invoicing*) and Schedule 8.1 (*Governance)* to be provided by the Supplier to the Director.

Material KPI Failure means:

(a) a Serious KPI Failure;

(b) a Severe KPI Failure; or

(c) a failure by the Supplier to meet a KPI Service Threshold.

Material PI Failure means:

(a) a failure by the Supplier to meet the PI Service Threshold in respect of twenty-five percent (25%) or more of the Subsidiary Performance Indicators that are measured in that Service Period; and/or

(b) a failure by the Supplier to meet the Target Performance Level in respect of fifty percent (50%) or more of the Subsidiary Performance Indicators that are measured in that Service Period.

Measurement Period means in relation to a Key Performance Indicator or Subsidiary Performance Indicator, the period over which the Supplier's performance is measured (for example, a Service Period if measured monthly or a twelve (12) month period if measured annually).

Milestone means an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date.

Milestone Achievement Certificate means the certificate to be granted by the Director when the Supplier has Achieved a Milestone, which shall be in substantially the same form as that set out in Annex 3 of Schedule 6.2 (*Testing Procedures*).

Milestone Date means the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved.

Milestone Payment means a payment identified in Schedule 7.1 (*Charges and Invoicing*) to be made following the issue of a Milestone Achievement Certificate.

Minor KPI Failure shall be as set out against the relevant Key Performance Indicator in Table 1 of Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Mobile Channel means the retail mobile device Channel, comprising of mobile apps and its supporting systems and services, enabling mobile access to publicly available Product and general information, and Digital Self-Service for Authenticated Customers.

Monitored Suppliers has the meaning given in Paragraph 5.3 of Schedule 7.4 (*Financial Distress*).

month means a calendar month and "**monthly**" shall be interpreted accordingly.

Multi-Party Dispute Resolution Procedure has the meaning given in Paragraph 8.1 of Schedule 8.3 (*Dispute Resolution Procedure*).

Multi-Party Procedure Initiation Notice has the meaning given in Paragraph 8.3 of Schedule 8.3 (*Dispute Resolution Procedure*).

NCSC means the National Cyber Security Centre or any replacement or successor body carrying out the same function.

New Releases means an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item.

Non-trivial Customer Base means a significant Customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor.

Non-retained Deliverables in relation to a CPP Milestone Payment Notice and each CPP Milestone the subject of that CPP Milestone Payment Notice, Deliverables provided to the Director which relate to the relevant CPP Milestone(s) and which are not Retained Deliverables.

Notifiable Default shall have the meaning given in Clause 29.1 *(Rectification Plan Process).*

Object Code means Software and/or data in machine-readable, compiled object code form.

Occasion of Tax Non-Compliance means:

(a) any tax return of the Supplier submitted to a Relevant Tax Director on or after 1st October 2012 is found on or after 1st April 2013 to be incorrect as a result of:

(i) a Relevant Tax Director 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; and/or

(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 Director under the DOTAS or any equivalent or similar regime; and/or

(b) any tax return of the Supplier submitted to a Relevant Tax Director on or after 1st October 2012 gives rise on or after 1st April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a civil penalty for fraud or evasion.

Open Book Data has the meaning given in Schedule 7.5 (*Financial Reports, Audit and Risk*).

Open Source means computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source.

Operating Environment means the Director System and the Sites.

Operational Service Commencement Date (or **OSCD**) in relation to an Operational Service, the later of:

(a) the date identified in the Operational Services Implementation Plan upon which the Operational Service is to commence; and

(b) where the Implementation Plan states that the Supplier must have Achieved the relevant ATP Milestone before it can commence the provision of that Operational Service, the date upon which the Supplier Achieves the relevant ATP Milestone.

Operational Services means the operational services described as such in the Services Description.

Other Supplier means any supplier to the Director (other than the Supplier) which is notified to the Supplier from time to time and/or of which the Supplier should have been aware.

Outline Implementation Plan means the outline plan set out at Annex 1 of Schedule 6.1 (*Implementation Plan*).

Overhead has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

Parent Undertaking has the meaning set out in section 1162 of the Companies Act 2006.

Partial Termination means the partial termination of this Agreement to the extent that it relates to the provision of any part of the Services as further provided for in Clause 35.2.2 (*Termination by the Director*) or 35.3 (*Termination by the Supplier*) or otherwise by mutual agreement by the Parties.

Parties and **Party** have the meanings respectively given on page 4 of this Agreement.

Performance Failure means a KPI Failure or a PI Failure.

Performance Indicators means the Key Performance Indicators and the Subsidiary Performance Indicators.

Permitted Maintenance has the meaning given in Clause 9.4 (*Maintenance*).

Performance Monitoring Report has the meaning given in Schedule 2.2 (*Performance Levels*).

Personal Data has the meaning given in the UK GDPR.

Personal Data Breach has the meaning given in the UK GDPR.

PI Failure means a failure to meet the Target Performance Level in respect of a Subsidiary Performance Indicator.

PI Service Threshold shall be as set out against the relevant Subsidiary Performance Indicator in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Premium Bond means the Director's Premium Bond product offering available to Customers.

Pricing Response Template is as appended at Annex 1 of Schedule 7.1 (*Charges and Invoicing*).

Processor has the meaning given to it under the UK GDPR.

Processor Personnel means all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Agreement.

Product means a financial services product (defined by its Product Terms and Conditions) offered to or held by Customers, which may be on-sale to Customers, temporarily withdrawn from sale (off-sale) or permanently withdrawn from sale (closed). A Product may have a number of issues, which may vary in duration and interest rate, but shall be deemed to be one Product.

Product Terms and Conditions means the set of terms and conditions that apply to a particular Product.

Prohibited Act means:

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Director a financial or other advantage to:

(i) induce that person to perform improperly a relevant function or activity; or

(ii) reward that person for improper performance of a relevant function or activity;

(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Agreement;

(c) an offence:

(i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act);

(ii) under legislation or common law concerning fraudulent acts; or

(iii) defrauding, attempting to defraud or conspiring to defraud the Director (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK.

Protective Measures means appropriate technical and organisational measures which may include but is not limited to: 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 such measures adopted by it.

Project Specific IPRs means:

(a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Agreement and updates and amendments of these items including (but not limited to) database schema; and/or

(b) Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Agreement;

but shall not include the Supplier Background IPRs or the Specially Written Software.

Public Retail Website means the Customer-facing website, containing publicly available Product and general information (also known as the marketing website).

Public Sector Dependent Supplier means a supplier where that supplier, or that supplier's group has Annual Revenue of £50,000,000 (fifty million pounds) or more of which over fifty percent (50%) is generated from UK Public Sector Business.

Public Sector and CNI Contract Information means the information requirements set out in accordance with Paragraphs 2 to 4 and Annex 2 of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

Publishable Performance Information means any of the information in the Performance Monitoring Report as it relates to a Performance Indicator where it is expressed as publishable in the tables in Annex 1 of Schedule 2.2 (*Performance Levels*) which shall not constitute Commercially Sensitive Information.

Quality Plans has the meaning given in Clause 6.1 (*Quality Plans*).

Quarter means the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall end on the date of termination or expiry of this Agreement).

Real Living Wage means the UK wage rate calculated according to the actual costs of living, as monitored, certified and updated from time to time by the Living Wage Foundation (https://www.livingwage.org.uk/what-real-living-wage).

Recipient has the meaning given in Clause 23.1 (*Confidentiality*).

Records has the meaning given in Schedule 8.4 (*Reports and Records Provisions*).

Rectification Plan means a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default.

Rectification Plan Failure means:

(a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Director within the timescales specified in Clauses 29.5 (*Submission of the draft Rectification Plan*) or 29.11 (*Agreement of the Rectification Plan*);

(b) the Director rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 20.10 (*Agreement of the Rectification Plan*);

(c) the Supplier failing to rectify a material Default which is capable of remedy within the later of:

(i) thirty (30) Working Days of a notification made pursuant to Clause 29.2 *(Notification)*; and

(ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default;

(d) the Supplier failing to start the Rectification Plan in accordance with Clause 29.13.1;

(e) a Material KPI Failure re-occurring in respect of the same Key Performance Indicator for the same (or substantially the same) root cause in any of the three (3) Measurement Periods subsequent to the Measurement Period in which the initial Material KPI Failure occurred;

(f) the Supplier not Achieving a Key Milestone by the revised date identified in the Rectification Plan;

(g) the Supplier committing a Default which is incapable of remedy; and/or

(h) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of six (6) months for the same (or substantially the same) root cause as that of the original Notifiable Default.

Rectification Plan Process means the process set out in Clauses 29.5 (*Submission of the draft Rectification Plan*) to 29.10 (*Agreement of the Rectification Plan*).

Registers has the meaning given in Schedule 8.5 (*Exit Management*).

Reimbursable Expenses has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

Related Services means those services being delivered by Relevant Third Party Suppliers as part of the End to End Service.

Relevant Authority or **Relevant Authorities** means the Director and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team.

Relevant IPRs means IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Director or a third party in the fulfilment of the Supplier's obligations under this Agreement including IPRs in the Specially Written Software, the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third Party Non-COTS Software and the Third Party Non-COTS IPRs but excluding any IPRs in the Director Software, the Director Background IPRs, the Trade Marks, the Supplier COTS Software, the Supplier COTS Background IPRS, the Third Party COTS Software and/or the Third Party COTS IPRs.

Relevant Requirements means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010.

Relevant Tax Authority means HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established.

Relevant Third Party Supplier means a third party supplier providing Related Services.

Relevant Transfer means a transfer of employment to which the Employment Regulations applies.

Relief Notice has the meaning given in Clause 33.2 (*Director Cause*).

Remedial Adviser means the person appointed pursuant to Clause 31.2 (*Remedial Adviser*).

Remedial Adviser Failure has the meaning given in Clause 31.9 (*Remedial Adviser*).

Replacement Services means any services which are the same as or substantially similar to any of the Services and which the Director receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Agreement, whether those services are provided by the Director internally and/or by any third party.

Replacement Supplier means any third party service provider of Replacement Services appointed by the Director from time to time (or where the Director is providing Replacement Services for its own account, the Director).

Request For Information means a Request for Information under the FOIA or the EIRs.

Required Action has the meaning given in Clause 32.1.1 (*Step-In Rights*).

Retained Deliverables has the meaning given in Clause 36.8 (*Payments by the Supplier*).

Risk Data means the data relating to risk including key risks and controls, open audit actions and results of control testing, which the Supplier is required to deliver to the Director under Part 4 of Schedule 7.5 (*Financial Reports, Audit and Risk*).

Risk Register means the register of risks and contingencies as created and maintained by the Supplier during the Term of this Agreement.

Secure Message means digital messaging between the Director and Authenticated Customers via the Authenticated Retail Website and/or Mobile Channel.

Security Management Plan means the Supplier's security plan as attached as Annex 3 of Schedule 2.4 (*Security Management*) and as subsequently developed and revised pursuant to Paragraphs 6 and 7 of Schedule 2.4 (*Security Management*).

Serious KPI Failure shall be as set out against the relevant Key Performance Indicator in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Service Charges means the periodic payments made in accordance with Schedule 7.1 (*Charges and Invoicing*) in respect of the supply of the Operational Services.

Service Continuity Plan means any plan prepared pursuant to Paragraph 2 of Part 1 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*) as may be amended from time to time.

Service Continuity Services means the business continuity, disaster recovery and insolvency continuity services set out in Part 1 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

Service Credit Cap means:

(a) in the period of twelve (12) months from the first Operational Service Commencement Date to occur after the Effective Date, [redacted] of the Estimated Initial Service Charges; and

(b) during the remainder of the Term, [redacted] of the Service Charges paid and/or due to be paid to the Supplier under this Agreement in the period of twelve (12) months immediately preceding the Service Period in respect of which Service Credits are accrued.

Service Credits means credits payable by the Supplier due to the occurrence of one (1) or more KPI Failures, calculated in accordance with Paragraph 3 of Part 3 of Schedule 7.1 (*Charges and Invoicing*).

Service Desk means the overarching Incident (as defined in Schedule 2.2 (*Performance Levels*)) management service provided by or on behalf of the Director (including by a nominated Relevant Third Party Supplier) across the End to End Service.

Service Period means a calendar month, save that:

(a) the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and

(b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term.

Service Points in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Services means any and all of the services to be provided by the Supplier under this Agreement, including those set out in Schedule 2.1 (*Services Description*).

Service Recipients means any individual, Customer or other organisation which receives Services including recipients of the B2B Services.

Service Transfer Date has the meaning given in Schedule 9.1 (*Staff Transfer*).

Services Description means the services description set out in Schedule 2.1 (*Services Description*).

Severe KPI Failure shall be as set out against the relevant Key Performance Indicator in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Sites means any premises (including the Director Premises, the Supplier's premises, Relevant Third Party Suppliers or other third party premises):

(a) from, to or at which:

(i) the Services are (or are to be) provided; or

(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or

(iii) the Supplier Equipment is used or deployed; or

(b) where:

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Director System takes place.

SME means 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.

Social Value means the social, economic or environmental benefits set out in the Director's Requirements.

Software means Specially Written Software, Supplier Software and Third Party Software.

Software Supporting Materials has the meaning given in Clause 17.1.1(b) (*Specially Written Software and Project Specific IPRs*).

Source Code means 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 related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such Software.

Specially Written Software means any Software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-contractor or other third party on behalf of the Supplier) specifically for the purposes of this Agreement, including any modifications or enhancements to Supplier Software or Third Party Software created specifically for the purposes of this Agreement.

Specific Change in Law means a Change in Law that relates specifically to the business of the Director and which would not affect a Comparable Supply.

Staffing Information has the meaning given in Schedule 9.1 (*Staff Transfer*).

Standards means the standards, polices and/or procedures identified in Schedule 2.3 (*Standards*).

Standard Contractual Clauses means the clauses set out in Annex 1 of Schedule 11 (*Processing Personal Data*).

Step-In Notice has the meaning given in Clause 32.1 (*Step-In Rights*).

Step-In Trigger Event means:

(a) any event falling within the definition of a Supplier Termination Event;

(b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services;

(c) the Director considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Agreement;

(d) the Director being advised by a regulatory body that the exercise by the Director of its rights under Clause 32 (*Step-In Rights*) is necessary;

(e) the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or

(f) a need by the Director to take action to discharge a statutory duty.

Step-Out Date has the meaning given in Clause 32.5.2 (*Step-In Rights*).

Step-Out Notice has the meaning given in Clause 32.5 (*Step-In Rights*).

Step-Out Plan has the meaning given in Clause 32.6 (*Step-In Rights*).

Strategic Supplier means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers.

Sub-contract means any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof.

Sub-contractor means any third party with whom:

(a) the Supplier enters into a Sub-contract; or

(b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party.

Sub-contractor Group means the Sub-contractor, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings.

Sub-processor means any third party appointed to process Personal Data on behalf of the Supplier related to this Agreement.

Subsidiary Performance Indicator means the performance indicators identified as such and set out in the table in Part 1 of Annex 1 of Schedule 2.2 (*Performance Levels*).

Subsidiary Undertaking has the meaning set out in section 1162 of the Companies Act 2006.

Successor Body has the meaning given in Clause 38.4 *(Assignment and Novation)*.

Supplier Background IPRs means:

(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer programming or in physical or electronic media containing the Supplier's Know-How or generic business methodologies; and/or

(b) Intellectual Property Rights created by the Supplier independently of this Agreement,

which in each case is or will be used before or during the Term for designing, testing, implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software.

Supplier COTS Background IPRs means any embodiments of Supplier Background IPRs that:

(a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and

(b) has a Non-trivial Customer Base.

Supplier COTS Software means Supplier Software (including Open Source software) that:

(a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and

(b) has a Non-trivial Customer Base.

Supplier Equipment means the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Director) for the provision of the Services.

Supplier Group means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings.

Supplier Non-COTS Background IPRs means any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Director and that are not Supplier COTS Background IPRs.

Supplier Non-COTS Software means Supplier Software that is not Supplier COTS Software.

Supplier Non-Performance has the meaning given in Clause 33.1 (*Director Cause*).

Supplier Personnel means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-contractor engaged in the performance of the Supplier's obligations under this Agreement.

Supplier Profit has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

Supplier Profit Margin has the meaning given in Schedule 7.1 (*Charges and Invoicing*).

Supplier Representative means the representative appointed by the Supplier pursuant to Clause 11.3 (*Representatives*).

Supplier Software means Software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including the Software specified as such in Schedule 5.1 (*Software*).

Supplier Solution means the Supplier's solution for the Services set out in Schedule 4.1 (*Supplier Solution*) including any Annexes of that Schedule.

Supplier System means the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Director System).

Supplier Termination Event means:

(a) the Supplier's level of performance constituting a Critical Performance Failure;

(b) the Supplier committing a material Default which is irremediable;

(c) as a result of the Supplier's Default, the Director incurring Losses in any Contract Year which exceed eighty percent (80%) of the value of the aggregate annual liability cap for that Contract Year as set out in Clause 27.6.2 (*Financial and other Limits*);

(d) a Remedial Adviser Failure;

(e) a Rectification Plan Failure;

(f) where a right of termination is expressly reserved in this Agreement, including pursuant to:

(i) Clause 20 (*IPRs Indemnity*);

(ii) Clause 41.6.2 (*Prevention of Fraud and Bribery*);

(iii) Paragraph 6 of Schedule 7.4 (*Financial Distress*); and/or

(iv) Paragraph 2 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

(g) the representation and warranty given by the Supplier pursuant to Clause 3.2.9 (*Warranties*) being materially untrue or misleading;

(h) the Supplier committing a material Default under Clause 10.10 (*Promoting Tax Compliance*) or failing to provide details of steps being taken and mitigating factors pursuant to Clause 10.10 (*Promoting Tax Compliance*) which in the reasonable opinion of the Director are acceptable;

(i) the Supplier committing a material Default under any of the following Clauses:

(i) Clause 5.6.10 (*Services*);

(ii) Clause 25 (*Protection of Personal Data*);

(iii) Clause 24 (*Transparency and Freedom of Information*);

(iv) Clause 23 (*Confidentiality*); and

(v) Clause 37 (*Compliance*); and/or

(vi) in respect of any security requirements set out in Schedule 2.1 (*Services Description*), Schedule 2.4 (*Security Management*) or the Baseline Security Requirements; and/or

(vii) in respect of any requirements set out in Schedule 9.1 (*Staff Transfer*);

(j) any failure by the Supplier to implement the changes set out in a Benchmark Report as referred to in Paragraph 5.9 of Schedule 7.3 (*Benchmarking*);

(k) an Insolvency Event occurring in respect of the Supplier or the Guarantor;

(l) the Guarantee ceasing to be valid or enforceable for any reason (without the Guarantee being replaced with a comparable guarantee to the satisfaction of the Director with the Guarantor or with another guarantor which is acceptable to the Director);

(m) a change of Control of the Supplier or a Guarantor unless:

(i) the Director has given its prior written consent to the particular Change of Control, which subsequently takes place as proposed; or

(ii) the Director has not served its notice of objection within six (6) months of the later of the date on which the Change of Control took place or the date on which the Director was given notice of the Change of Control;

(n) a change of Control of a Key Sub-contractor unless, within six (6) months of being notified by the Director that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Director pursuant to Clause 15.10 (*Appointment of Key Sub-contractors*);

(o) any failure by the Supplier to enter into or to comply with an Admission Agreement under the Annex to Part 4 or Part 5 of Schedule 9.1 (*Staff Transfer*);

(p) the Director has become aware that the Supplier should have been excluded under Regulation 57(1) or (2) of the Public Contracts Regulations 2015 from the procurement procedure leading to the award of this Agreement;

(q) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law;

(r) in relation to Schedule 2.4 (*Security Requirements*):

(i) the Director has issued two rejection notices in respect of the Security Management Plan under Paragraph 6.5.2;

(ii) the Supplier fails to implement a change required by the Required Changes Register in accordance with the timescales set out in the Required Changes Register;

(iii) Supplier COTS Software and Third Party COTS Software is not within mainstream support unless the Director has agreed in writing;

(iv) the Supplier fails to patch vulnerabilities in accordance with the Security Requirements; and/or,

(v) the Supplier fails to comply with the Incident Management Process; or

(s) a failure to meet a Long Stop Date in accordance with Schedule 6.1 (*Implementation Plan*).

Supply Chain Transparency Report means the report provided by the Supplier to the Director in the form set out in Annex 4 of Schedule 8.4 (*Reports and Records Provisions*).

Target Performance Level means the minimum level of performance for a Performance Indicator which is required by the Director, as set out against the relevant Performance Indicator in the tables in Annex 1 of Schedule 2.2 (*Performance Levels*).

Term means the period commencing on the Effective Date and ending on the expiry of the Initial Term, any Extension Period, or the Termination Assistance Period (whichever is later), or on earlier termination of this Agreement.

Termination Assistance Notice has the meaning given in Paragraph 5.1 of Schedule 8.5 (*Exit Management*).

Termination Assistance Period in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination

Services as such period may be extended pursuant to Paragraph 5.3 of Schedule 8.5 (*Exit Management*).

Termination Date means the date set out in a Termination Notice on which this Agreement (or a part of it as the case may be) is to terminate.

Termination Notice means a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Agreement (or any part thereof) on a specified date and setting out the grounds for termination.

Termination Payment means the payment determined in accordance with Schedule 7.2 (*Payments on Termination*).

Termination Services means the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 8.5 (*Exit Management*), and any other services required pursuant to the Termination Assistance Notice.

Test Issues has the meaning given in Schedule 6.2 (*Testing Procedures*).

Tests and **Testing** means any tests required to be carried out under this Agreement, as further described in Schedule 6.2 (*Testing Procedures*) and "**Tested**" shall be construed accordingly.

Test Success Criteria has the meaning given in Schedule 6.2 (*Testing Procedures*).

Third Party Auditor means an independent third party auditor as appointed by the Director from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in Schedule 8.4 (*Reports and Records Provisions*).

Third Party Beneficiary has the meaning given in Clause 46.1 (*Third Party Rights*).

Third Party Contract means those third party contracts which the Supplier enters into exclusively for the purpose of delivering the Services, as set out in Schedule 4.4 (*Third Party Contracts*).

Third Party COTS IPRs means Third Party IPRs that:

(a) the supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and

(b) has a Non-trivial Customer Base.

Third Party COTS Software means Third Party Software (including Open Source software) that:

(a) the supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and

(b) has a Non-trivial Customer base.

Third Party IPRs means Intellectual Property Rights owned by a third party but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software.

Third Party Non-COTS IPRs means Third Party IPRs that are not Third Party COTS IPRs.

Third Party Non-COTS Software means Third Party Software that is not Third Party COTS Software.

Third Party Provisions has the meaning given in Clause 46.1 (*Third Party Rights*).

Third Party Software means software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the Software specified as such in Schedule 5 (*Software*).

Touchpoint (or **touchpoints**) means an interaction between the Customer and the Director through an exchange of information, provision of a service or undertaking of a transaction via a Channel and using a device, e.g. withdrawing money via the mobile app on a mobile device.

Trade Mark means each of the registered trade marks owned by the Director, as set out in the Trade Mark Licence, or notified to the Supplier from time to time and those unregistered trade marks owned by the Director as agreed in writing by the Director to be within scope of the Trade Mark Licence from time to time, and "**Trade Marks**" shall be construed accordingly.

Trade Mark Licence means the terms of the licence granted by the Director to the Supplier for use of the Trade Marks pursuant to Clause 19 (*Licences Granted by the Director*) and those terms set out in Schedule 5.2 (*Trade Mark Licence Terms*).

Transferring Assets has the meaning given in Paragraph 6.2.1 of Schedule 8.5 (*Exit Management*).

Transferring Director Employees has the meaning given in Schedule 9.1 (*Staff Transfer*).

Transferring Former Supplier Employees has the meaning given in Schedule 9.1 (*Staff Transfer*).

Transferring Services means the Services to transfer to the Director or a Replacement Supplier in accordance with Schedule 8.5 (*Exit Management*).

Transferring Supplier Employees has the meaning given in Schedule 9.1 (*Staff Transfer*).

Transformation Committee has the meaning given in Schedule 8.1 (*Governance*).

Transparency Information has the meaning given in Clause 24.1 (*Transparency and Freedom of Information*).

Transparency Reports has the meaning given in Schedule 8.4 (*Reports and Records Provisions*).

UK means the United Kingdom.

UK GDPR means the retained EU law version of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018.

UK Public Sector Business means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations.

UK Public Sector / CNI Contract Information means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 2 to 4 and Annex 2 of Part 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

Unacceptable KPI Failure means the Supplier failing to achieve the KPI Service Threshold in respect of more than twenty (20%) of the Key Performance Indicators that are measured in that Service Period.

Unconnected Sub-contract means any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying

contract under regulation 6 of The Reporting on Payment Practices and Performance Regulations 2017.

Unconnected Sub-contractor means any third party with whom the Supplier enters into an Unconnected Sub-contract.

Updates in relation to any Software and/or any Deliverable means a version of such item which has been produced primarily to overcome Defects in, or to improve the operation of, that item.

Update Requirement means the occurrence of an event detailed in Schedule 8.4 (*Reports and Records Provisions*), Annex 3 (*Virtual Library*) which requires the Supplier to update the relevant information hosted on the Virtual Library.

Upgrades means any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term.

User means any person who is an authorised end user of the Services, the Supplier's System or other information system or application required to be provided as set out in the Director's Requirements.

Valid in respect of an Assurance, has the meaning given to it in Paragraph 1.7 of Part 2 to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*).

VAT means value added tax as provided for in the Value Added Tax Act 1994.

VCSE means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

Virtual Library means the data repository hosted by the Supplier containing the information about this Agreement and the Services provided under it in accordance with Schedule 8.4 (*Reports and Records Provisions*).

Working Day means any day other than a Saturday, Sunday or public holiday in England and Wales.

SCHEDULE 2.1 - SERVICES DESCRIPTION

1 INTRODUCTION

1.1 This Schedule 2.1 (*Services Description*) sets out the background and intended scope of the Services to be provided by the Supplier and to provide a description of what each Service entails.

2 BACKGROUND TO THE DIRECTOR

2.1 The Director is an Executive Agency of the Chancellor of the Exchequer. It is one of the UK's largest retail savings organisations with 25 million customer and more than £202 billion of funds under management, best known for Premium Bonds but also offering a wide range of other savings products. The Director's remit is to raise cost-effective financing for Government. This is achieved by offering a range of secure retain financial savings products, as an alternative to raising funds on the wholesale market.

3 BACKGROUND TO RAINBOW

3.1 The Director's core services are currently provided by Atos IT Services UK Limited, which manages sales processing and customer servicing, in addition to IT and infrastructure services ("**Legacy Services Contract**"). This contract is due to expire on 31st March 2025.

3.2 The Director is embarking on a significant programme of transformation for its outsourced services, called the Rainbow Programme. This procurement exercise, for Customer Contact and Operations Services, forms part of the Rainbow Programme.

3.3 The Director aims to become a self-service digital business with lower running costs and improved technical operational resilience. The Rainbow Programme will ensure the Director operates safely and can respond in a nimble, proactive way to changes in policy or the market and deliver the scale of business, in terms of holdings, customers and accounts it may be required to support in the coming years. This will involve a series of procurement processes to deliver transformational activities through new outsourcing contracts – and this Agreement for Customer Contact and Operations Services is one of these.

4 SERVICES DESCRIPTION

4.1 The Services to be provided under this Agreement are focused around Customer Contact Centre and Operations. The Director wished to procure a strategic supplier of managed services to support, deliver and integrate contact centre services, including the provision of Assisted Digital capabilities, supporting Customers through digital self-service and Customer journeys that may be performed on their behalf, particularly when needed to support vulnerable and digitally excluded Customers.

4.2 The selected Supplier is to provide the people, relevant contact centre technology and capabilities to enable and manage the Director's assisted digital Customer journeys and experiences. It will request and support data provision and insight from these Services to be shared with the Director's other Relevant Third Party Providers to both inform the organisation's digital Customer journeys and experiences and to build its Knowledge and Insight capabilities. The Supplier shall also deliver operational "back-office" capabilities and services, including complaints management, to manage and process non-digital Customer interactions and journeys.

4.3 While 96% of the Director's Customer interactions originate from digital channels, with 6 million customers registered to use online, responses and out bound services currently have lower levels of digital origination. The Director's aspiration is for Customers to digitally self-serve and while the organisation is on the journey to achieve this, the Supplier will need to have capabilities to accept and scan post with integrated services into the back-office processes/capabilities as well as print capabilities for outbound services.

4.4 Reviewing, redesigning and reducing non-digitised interactions and journeys while improving efficiency and reducing Customer effort will be vital. Actionable insight will need to be gathered and

used to help identify such non-digital interactions/journeys that could be digitised and/or automated ensuring more digital self-serve Customer journeys are enabled. This may include for example identifying and implementing opportunities for robotic automation.

4.5 The Implementation Services include those services to be provided by the Supplier for the design, build, test, transition, implementation and roll out of the Operational Services including as set out in the Implementation Plan provided pursuant to Schedule 6.1 (*Implementation Plan*).

4.6 At a high level and notwithstanding the Statement of Requirements (in Annex 1) or the Supplier Solution in Schedule 4.1, the Operational Services at a high level include:

4.6.1 Contact Centre;

4.6.2 back office;

4.6.3 document management;

4.6.4 mail-in scanning;

4.6.5 print and dispatch.

4.7 The Operational Services will be brought in through a phased approach in accordance with the Operational Service Commencement Dates identified in the Implementation Plan.

4.8 The Director Requirements in relation to Implementation Services and Operational Services are described in more detail in the following Annexes to this Schedule:

4.8.1 Annex 1: Statement of Requirements - V2_Feb23;

4.8.2 Annex 2: Requirements Catalogue V1.1.

4.9 The Director Requirements include, at a high level the following categories:

4.9.1 Contact Centre

(a) Contact Centre as a Service

(b) Customer response

(c) Assisted Digital capabilities

(d) Acting on behalf of Customers unwilling or unable to use digital self-serve channels

4.9.2 Non-digitised Processing

(a) Efficient Customer journey design

(b) Customer Complaint Handling

(c) Staff and sites

(d) Financial Crime team

4.9.3 Document Management

(a) Centralised mail hub, pick up and postage

(b) Scanning and OCR

(c) Cheque banking

(d) Centralised print

(e) Document storage and view, document retrieval

(f) Template management, document creation

4.9.4 Architecture and Integration – provide a secure and reliable infrastructure delivering the Contract Centres and non-digital customer elements. The Director's customers need all elements of the Services to be trustworthy and reliable:

(a) Secure and reliable infrastructure

(b) Alignment with Director's design principles & regulatory requirements

(c) Risk and assurance framework

4.9.5 Ways of Working

(a) Iterative and data-driven service improvements

(b) Design and development with competitor, service and customer intelligence

(c) "Always on" continuous improvement approach

4.10 Collaboration – the Supplier will be required to collaborate and work alongside other suppliers appointed as part of the Rainbow Programme. Specific obligations with regard to this collaborative approach are set out in Schedule 12 (*Collaboration Agreement*).

4.11 Contact Centre – the above committed services described in Paragraph 4 and in more detail in Annex 1 includes the transition, design, build, deployment and operation of the Services during the Term, including integration into the digital integration platform and where applicable with the Legacy Services Contract provision.

5 ADDITIONAL SERVICES

5.1 Subject to the above Paragraph 4, the Parties acknowledge that:

5.1.1 Additional Services may include future integrations including the on-boarding of:

(a) Relevant Third Party Suppliers; and

(b) Suppliers delivering the B2B Services;

5.1.2 Adding new B2B Services beyond the scope of the B2B Services delivered at the Effective Date shall be deemed Additional Services; and

5.1.3 Any Additional Services required by the Director shall be subject to the provisions of Clauses 5.11 to 5.14 of the Agreement.

Annex 1: Statement of Requirements

Schedule 21 Services Description Annex 1 Statement of Requirements - V_Feb23 PDF (48361918.1).pdf.pdf

Annex 2: Requirements Catalogue

Schedule 2.1 Services Description Annex 2 Requirements Catalogue V1.1 FINAL (48361949.1).xlsx.nrl.xlsx

COMPETITIVE DIALOGUE PROCEDURE

FOR

CUSTOMER CONTACT AND OPERATIONS

VOLUME 2

STATEMENT OF REQUIREMENTS

VERSION 2.0

Important Notices

Please read this document first, before attempting to respond to the opportunity.

This "Statement of Requirements" document has been prepared by National Savings & Investments ("the Director") and is for the use of those entities intending to bid to deliver the Project, their professional advisers and other parties essential to preparing their Selection Questionnaire responses and Bids, and for no other purpose.

You are deemed to fully understand the process that the Director is required to follow under relevant UK (and retained European law) particularly in relation to the public procurement rules.

Your attention is drawn to the notices set out in Appendix 1 (Procurement Conditions) which form part of the conditions for participation that apply to Candidates and Bidders in this procurement process.

Table of contents

1. INTRODUCTION 3
2. CONTEXT 4
3. CUSTOMER CONTACT AND OPERATIONS 7
4. OVERVIEW OF REQUIREMENTS 12
5. CHANGES FROM PREVIOUS VERSION 42
6. APPENDICES 51

VOLUME 2 – SECTION 1

STATEMENT OF REQUIREMENTS for SERVICES SOUGHT

1. Introduction

The Transition State 3 Project in NS&I's Rainbow programme, Customer Contact and Operations package will deliver new capabilities for the customer contact centre and operations processing for NS&I. It will provide Assisted Digital service to support NS&I's customers who are unable to complete their interactions via digital self-service, answer their general and complex enquiries. It will service non-digitised processing, streamline these processes and automate where appropriate. It will operate Financial Crime management, Document Management, Print and Post in/out services and will manage any customer complaints.

1.1 Capabilities

The capabilities comprise of a contact centre, ways of working, and technology.

1.1.1. Contact Centre

Skills and resources to provide:

- Contact Centre to seamlessly manage the customer interactions where services are not yet fully digitised or customers who are unable to complete their interactions via digital self-service
- Operations functions to process non-digitised / non automated activity
- Complaints and Incident Management

1.1.2. Ways of Working

Best practice ways of working through:

- Resource forecasting, planning, and scheduling based on contact demands
- Monitoring performance, providing feedback and actionable insights
- Learning and development of Customer Contact and Operations Centre staff.

1.1.3. Non-Digitised Operations

A managed service solution including but not limited to:

- The integration of the Contact Centre and non-digitised Middle/Back Office processing, as well as the sites needed to operate from.
- Case Management and workflow solution
- Document Management, Post in/out, scanning/Print services
- Financial Crime management
- Data Analytics, Insights, MI and Reporting.

2. Context

2.1. Our vision

In 2026, NS&I is the UK's most trusted savings provider. We deliver securely and cost-effectively for customers and stakeholders.

2.2. The Rainbow programme

2.2.1 Rainbow Programme aims

- Reduce operating costs
- Become a self-service digital business
- Be scalable, flexible, and secure

2.2.2. Commercial model

BASE CONTRACT		FINAL CONTRACTS
Model Services Contract	NS&I amendments ➔	Digital integration and Service Ops
		Digital Experience and Digital Enablement
		Customer Contact and Operations
		Core Banking, Payments and Reporting

2.2.3. High-level transition states

1	**Enabling Technology**	Establish suitable technology to enable integration and management of new services
2	**Digital Customer Experience**	Create a modern digital-first customer experience with improved customer journeys based on Jobs to be Done
3	**Customer Contact**	Establish a seamless Assisted Digital service to customers
4	**Core Banking and Insight**	Deliver banking products on a modern digital banking platform; make insight-driven decisions
5	**Continual Improvement**	Decommission final legacy services and drive continual improvement

2.3 Our business

National Savings and Investments (NS&I) is one of the largest savings organisations in the UK with:

- Over **25 million** customers
- More than **£200 billion** invested
- **Six million** customers registered for online
- **4.6 million** paperless holdings
- **43.4 million** accounts with NS&I
- **96.4%** of incoming customer engagement is via digital channels (telephone, email & letter)

NS&I is both a government department and an Executive Agency of the Chancellor of the Exchequer. Our origins can be traced back 160 years to 1861.

When customers invest in NS&I products, they are lending to the Government. In return, the Government pays interest or prizes for Premium Bonds. We offer 100% security on all savings, backed by HM Treasury.

2.3.1. Gross inflows

2018-19	**£37.3 billion**
2019-20	**£38.2 billion**
APRIL-SEPTEMBER '20	**£52.9 billion**

2.3.2. Current service volumes

Premium Bonds

- c. **3 million** Premium Bonds prizes paid out monthly of which each month **c.300,000** are paid by warrant

Customer interactions

- **1 million** sales per month
- **700,000** withdrawals each month

Customer logins

- More than **3.5 million** people are active online customers
- Today these logins are web driven rather than app driven
- **2 million** unique logins every month

Term deposits

- **500,000–700,000** term deposits maturing every year
- Around **50,000** per month, sometimes peaking at over 3x that number

Contact Centre in 2021-22

- c. **3.2 million** calls received

- c. **1.3 million** chats, of which 93% were answered by bot

Mail In 2021-22

- c.**119,000** cheques received
- c.**233,000** cherished document received and sent back
- c. **1.4 million** items of post

Print and Post Out 2021-22

- c.**16.4 million** output packs sent
- Of which, c.**1.1 million** are Annual statements

2.3.3. Further information

- For more information on NS&I's products and services - nsandi.com
- Further insight into NS&I's performance as a business - Our performance

2.4 2026 vision

NS&I's 2026 vision is:

> *In 2026, NS&I is the UK's most trusted savings provider. We deliver securely and cost-effectively for customers and stakeholders*

In support of the 2026 Vision, the Rainbow programme has 3 core aims:

- Delivering a measurable reduction to the cost of running and changing the business
- Becoming a self-service digital business with support for the vulnerable and excluded
- Delivering a more nimble, secure business, that reduces risk and enhances scalability

3. Customer Contact and Operations

3.1 Our aims for this package

3.1.1. What we need for our customers

- To support our customers with assisted digital services to assist with the complex enquiries
- To provide effective, cost-efficient support for customers unable or unwilling to self-serve digitally
- Improve customer experience through reduced processing times
- Improve customer experience through designing processes where the customer can be put back into the digital journey quickly

3.1.2. What we're looking for from our partners

- The Transition State 3 Project is the mechanism by which NS&I will introduce a new contact centre and back-office processing capability. The new services will be delivered by a new supplier / contract acquired via Procurement Package C (PPC).
- Key to achieving a successful outcome will be ensuring the integration of the contact centre and back-office operations with the Digital Self-serve Operations being delivered as part of Transition State 2 and Procurement Package B.
- This package will deliver capabilities which will change our approach to the customer contact centre and will be more focussed around helping customers to complete their tasks digitally (less paper contact) – including doing tasks for customers unable or unwilling to use digital channels. Contact centre staff will use the same facilities as provided to customers (with a more specialist user interface) to assist customers with most of their tasks. In collaboration with the digital experience provider, we will look to reduce customer and operational effort in simplifying and automating processes. When operational intervention is needed the journeys are designed to get the customer back into the digital journey as quickly as possible.
- This package will have a key role in transitioning non-digital customers to online, with communications, support throughout the journey. We welcome your ideas and solutions to help shape and drive this.
- You will need to identify actionable insights into customers behaviors, digital fallout and areas of friction to inform continuous improvement or automation and identify changes to journeys or processes, and all of this can only be achieved collaboratively with other providers, especially the digital customer experience provider.
- The supplier will need to support the vulnerable and digitally excluded customers
- As with all the packages we seek modern off the shelf solutions that are reusable and configurable, lowering the cost and increasing the speed of change which will be delivered iteratively.

Driving digital

Operations

Establish a seamless 'Assisted Digital' service to customers & automate processing where possible

Transitioning non-digital customers	Actionable Insight	Continuous improvement	Collaboration
Drive digital adoption	Reduce digital fall out	Increase Straight Through Processing	Support vulnerable and digitally excluded

Broader principles

Operations

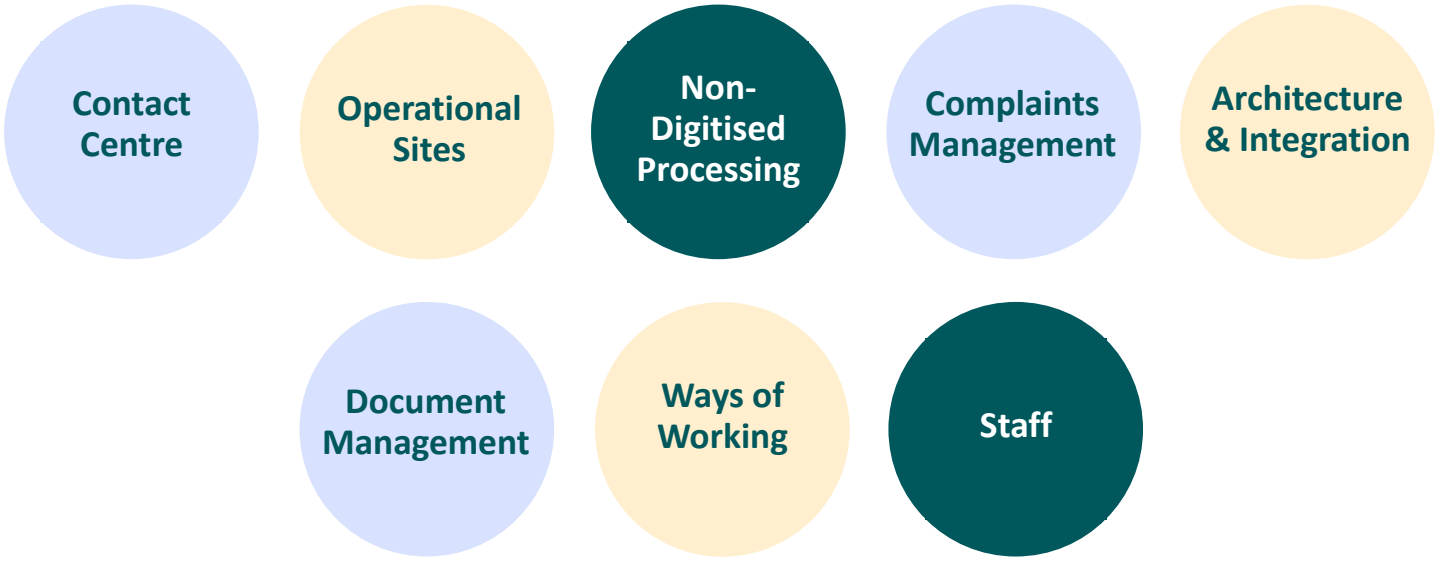
Reducing Customer and Operational effort, through the use of off-the-shelf solutions and capabilities to simplify processes and be able to assist customers through their digital journey when necessary

Off the shelf	Reusable	Configuration
Speed of change	Low cost of change	Iterative
Scalable	Resilient	Intelligent

3.2 Customer Contact and Operations - Requirements

For this package we have grouped the requirements into the main functional elements pertinent to the operation:

- This includes the staff required for the Contact Centre and non-digitised Middle/Back Office processing, as well as the sites needed to operate from.
- In the contact centre we need to have the capabilities and technologies to help customers who are struggling or need reassurance through their digital journey and act on behalf of those who are digitally excluded.
- For back office processing, where digital journeys need non digital intervention or decision, have processes designed to get the customer back into the digital journey as quick as possible with minimal customer and operational effort.
- When something has gone wrong for a customer and they complain, the co-ordination and management, as well as ensuring any issue is rectified quickly, is needed. This may require multiple supplier involvement as part of any complaint investigation and/or rectification.
- As we are only part way through our self-serve digital journey receiving, sorting and scanning the mail in and sending out paper documentation are scalable capabilities that are required, with the expectation that these will reduce over time.
- Architecture & Integration and the way we work collectively, are overarching in delivering these requirements in enabling access to relevant systems and provide a step change improvement in the way we deliver and how our customers experience NS&I.



3.2.1. Contact Centre

- Provide Contact Centre as a Service
- Providing staff with solutions that enable them to deal with a customer 'one and done'
- Responding to customers through various media
- Assisted digital capabilities such as co-browsing
- Acting on behalf of customers who are unwilling or unable to use digital self-serve channels

3.2.2. Non-digitised Processing

- Collaboration with other suppliers to ensure customer journeys and experiences are designed for all customer persona types
- Reducing customer effort by design, ensuring only necessary drops into non–digitised parts of the journey
- With customers being put back into the digital journey as quickly as possible
- Reduce operational effort in processing, identify and implement automation
- Customer Complaint Handling including those referred to NS&I via the Financial Ombudsman Service
- Staff and sites
- Financial Crime team

3.2.3. Document Management

- Centralised hub for Receiving Customer Mail
- Scanning and improving efficiency with technologies such as OCR
- Cheque Banking
- Actionable insight
- Scalability, up and down
- Centralised Print
- Mail Pick up and Postage
- Document storage and view
- Template management
- Document creation
- Print composition
- Document Retrieval

3.2.4. Architecture & Integration

Provide a Secure and reliable infrastructure delivering the Contact Centres and non-digital customer elements. Our customers need the elements above to be trustworthy and reliable. Together we'll need to assure:

- Customers' savings and data are safe from security threats and attacks
- The underlying infrastructure is secure, resilient, and scalable whilst undergoing continuous improvement

We'll do that through a risk and assurance framework – in particular:

- Designing and delivering services and their underlying infrastructure that align with NS&I design principles
- As a bank, complying with UK financial services legislation and guide frameworks.

3.3.5. Ways of working

Enabling the creation, management, and optimisation of NS&I services to customers by:

- Empowering our people to decide and act on services improvements in a data-driven and iterative way
- Supporting proposition design and development with competitor, service, and customer intelligence
- Developing, with our suppliers, an “always on” continuous improvement approach.

4. Overview of Requirements

The capabilities required within this package will change our approach to the Customer Contact Centre and will be more focussed around helping customers to complete their tasks digitally – including doing tasks for the customers unable or unwilling to use digital channels. Contact centre staff will use the same facilities as provided to the customers (with a more specialist user interface) to assist customers with most of their tasks. In collaboration with the digital experience supplier, we will look to reduce customer and operational effort in simplifying and automating processes. When non-digital operational intervention is needed, the journeys are designed to get the customer back into the digital journey as quickly as possible. Also, this package aims to deliver the capabilities required to support the completion of the non-digital operations.

Key to achieving a successful outcome will be ensuring the integration of the contact centre and back-office operations with the Digital Self-Serve Operations being delivered as part of Transition State 2 and Procurement Package B supplier.

This package comprises of twelve headline commissioning requirements as below.

4.1 Commissioning requirement themes

Contact Centre	**1**	Provide an Assisted Digital service for our customers in alignment with our defined NS&I Digital Self-service Journeys, so that NS&I Customers, unable to digitally self-serve, are able to fully access our products and services
Middle/Back Office	**2**	Provide any non-digital operational processing required to support the delivery of customer services, so that NS&I is able to deliver the full suite of services that our customers expect
	3	Provide a complaints management service in accordance with regulatory standards, so that we can ensure customers get the service they expect, and any failures in services are remediated
	4	Provide a document production, storage, and management service, so that NS&I can meet its accessibility obligations relating to digitally excluded / vulnerable customers
	5	Provide any non-digital Prize Draw related operational processing, so that all prizes are allocated, exceptions resolved, and customers notified
Architecture & Service	**6**	Operate its defined and agreed customer services in accordance with all relevant risk frameworks and compliance legislation, so that NS&I delivers a trustworthy and safe customer experience
	7	Work with the NS&I SIAM function and other suppliers to deliver our services, so that customers journeys are seamless across the multi-supplier model

	8	Operate in a manner which protects NS&I customers from security threats and attacks, so that NS&I's brand and reputation are maintained
	9	Develop and operate its services in accordance with NS&I architectural design standards, including utilisation of any prescribed technologies, so that NS&I remains architecturally coherent, and services can easily be re-procured in the future
Knowledge & Insights	**10**	Provide NS&I with relevant competitor, service, and customer intelligence, so that NS&I can continuously improve its propositions and services
Transformation	**11**	Promote adoption of digital services so that NS&I can move from current to future operating model.
Financial Crime	**12**	Provide financial crime investigation and management services, so that NS&I can meet obligations to protect its customers and minimise losses through fraudulent activity.

4.2 The Commissioning Requirements

1. **As the NS&I Business Owner, I want the supplier to provide an Assisted Digital service for our customers in alignment with our defined NS&I Digital Self-service Journeys, so that NS&I Customers, unable to digitally self-serve, are able to fully access our products and services**

What's the business need?

- To provide effective, cost-efficient fallback support for customers unable to self-serve digitally
- To enable vulnerable and digitally excluded customers or those unwilling to self serve to fully access our products and services
- To provide an Assisted Digital service for our customers

Who will use these capabilities?

- Contact Centre Agents
- The Director
- Customers
- Other Suppliers (PPB, PPD)
- Back Office Teams

How will this be delivered?

The supplier will provide the resources, systems, processes, and training needed to develop the required services in collaboration with NS&I and other Suppliers. Where necessary the supplier will implement and maintain the required system integrations across the technology landscape.

Scope of this requirement

Provide an Assisted Digital service so that our vulnerable, digitally excluded or those unwilling to self serve to fully access products have full access to our services and products.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-AD-001	**Assisted Digital**	The supplier shall provide a UK based, CCA accredited contact centre so that the assisted digital services can be delivered for the Director's customers who are unable to self-serve digitally.
PPCL2-AD-002	**Assisted Digital**	The supplier shall facilitate customers completing their Jobs To Be Done so that a customer can complete the journey with assistance from an agent completing interactions or elements of interactions.
PPCL2-AD-003	**Assisted Digital**	The supplier shall facilitate customers completing their Jobs To Be Done so that a customer can complete the journey with an agent completing interactions on their behalf.
PPCL2-AD-004	**Assisted Digital**	The supplier should provide a capability to identify whether a customer is vulnerable across channels so that the vulnerable customers can be assisted appropriately.
PPCL2-AD-005	**Assisted Digital**	The supplier shall provide core Assisted Digital services via multiple channels (such as Co-Browsing, Chatbot, Telephony, Social Media, etc) so that they are able to service the customers efficiently and create seamless positive customer experience including when customers move across the channels.
PPCL2-AD-006	**Assisted Digital**	The supplier shall provide any future proof Assisted Digital services and technologies (such as AI, ML, NLP, etc) via multiple channels so that they are able to service the customers efficiently and create positive customer experience.
PPCL2-AD-007	**Assisted Digital**	The supplier shall provide a telephony channel including IVR to support the delivery of assisted digital services so that the customers are able to engage with the Director via their channel of choice and complete their digital journeys.
PPCL2-AD-008	**Assisted Digital**	The supplier shall provide secure online communication secure chat to support the delivery of assisted digital services so that the customers are able to engage with the Director via their channel of choice to complete their digital journeys.
PPCL2-AD-009	**Assisted Digital**	The supplier shall provide an in-app call capability to the Director's mobile app so that customers can communicate securely with the Agents.
PPCL2-AD-011	**Assisted Digital**	The supplier shall provide support for customer payments in collaboration with other suppliers and in compliance with payment rules, regulations and policies so that the customers can make payment securely.

PPCL2-AD-012	**Assisted Digital**	The supplier shall ensure that all the customer conversations across digital and non-digital channels are responded to, in line with the Director's quality standards and content strategy so that customer's queries are resolved successfully, and they have positive engaging experience.
PPCL2-AD-013	**Assisted Digital**	The supplier must ensure that the contact centre agents have skills, tools, and access to data so that they can achieve closure with the customer interactions on a "one and done" basis.
PPCL2-AD-014	**Assisted Digital**	The supplier should provide the fully integrated Case management capability so that the agents can identify, monitor, manage and resolve customer cases.
PPCL2-AD-015	**Assisted Digital**	The supplier shall provide an automated solution for the customers and agents so that they are able to obtain answers to FAQs.
PPCL2-AD-016	**Assisted Digital**	The Supplier provide an automated solution for the agents so that they are able to obtain answers to FAQs.
PPCL2-AD-017	**Assisted Digital**	The supplier shall provide the tools and run processes to obtain and monitor customer feedback so that these inputs can be included when improving services and providing insights to the director.
PPCL2-AD-018	**Assisted Digital**	The supplier shall work collaboratively with other suppliers to deliver end to end customer journeys across all channels so that service expectations are met.

2. As the NS&I Business Owner, I want the supplier to provide any non-digital operational processing required to support the delivery of customer services, so that NS&I is able to deliver the full suite of services that our customers expect

What's the business need?

NS&I Contract Centre and Operations have an objective to move from labour-intensive, paper-based, back-office processing and controls to a point where services are digitised, manual back-office processing are undertaken on an exception's basis, and customer transactions can be completed with minimal customer and operational efforts.

Who uses it?

- Contact Centre Agents
- Back Office Teams
- Customers

How do we deliver it?

This requirement will be delivered by providing highly efficient human intervention where processes cannot or have not yet been digitised. Non-digitised process shall be automated where appropriate to ensure high efficiency and great customer experience.

Scope of this requirement

The delivery of customer interactions that are not provided through Digital Experience and Digital Enablement platform i.e. not yet digitised services.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-OPS-001	**Non-Digital Operational Processing**	The supplier shall accurately execute operational processing of customer journeys, for example but not limited to the processes specified below (in requirements 2 - 13) which cannot be completed with the digital processes within appropriate timelines so that customers are provided with positive engagement experience.
PPCL2-OPS-002	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Bereavement service, until such a point that, in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-003	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Sales service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.

PPCL2-OPS-004	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Payments service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-005	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Proxies (including but not limited to, Power of Attorney, Court of Protection, Trusts, Independent Financial Adviser) service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-006	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Tracing (including those from My Lost account) service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-007	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the General Correspondence service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-008	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Change of details service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-009	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Records Management service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-010	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Return Undelivered service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-011	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Evidence of Identity service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-012	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Registration service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be

		completed with minimal customer and operational effort.
PPCL2-OPS-013	**Non-Digital Operational Processing**	The supplier shall provide operational processing for the Forgotten Security service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.
PPCL2-OPS-014	**Non-Digital Operational Processing**	The supplier shall execute operational processing of all customer journeys on behalf of customers unable to self-serve digitally so that such customers can complete their jobs to be done.
PPCL2-OPS-015	**Non-Digital Operational Processing**	The supplier shall ensure consistency in customer engagement experience between digital and non-digital journeys so that the Director can ensure equivalent experience for all customers.
PPCL2-OPS-016	**Non-Digital Operational Processing**	The supplier shall ensure reliable integration with other supplier(s') systems so that the supplier can securely communicate with customers digitally in relation to their interactions.
PPCL2-OPS-017	**Non-Digital Operational Processing**	The supplier shall integrate secure messaging with Customer Contact Case Workflow Management to identify when a customer has responded so that the supplier knows action needs to be taken.
PPCL2-OPS-018	**Non-Digital Operational Processing**	The supplier shall design and provide appropriate means to meet customers' correspondence requirements in accordance with the Directors agreed approach so that the Director can effectively communicate to its customers.
PPCL2-OPS-019	**Non-Digital Operational Processing**	The supplier shall, in collaboration with other suppliers promptly provide data on request so that the Director can complete obligations such as HMT requests, parliamentary requests, data underpinning PI results, FOI etc. in a timely manner as agreed by the Director.
PPCL2-OPS-020	**Non-Digital Operational Processing**	The supplier shall, in collaboration with other suppliers, ensure customer journeys which cannot be completed in the digitised services are easily transitioned to operational processing for completion so that customer journeys can be completed efficiently with minimal disruption.
PPCL2-OPS-021	**Non-Digital Operational Processing**	The supplier shall automate non-digitised processes where appropriate so that operational processing can be completed in an optimal manner.
PPCL2-OPS-022	**Non-Digital Operational Processing**	The supplier shall apply the following principles, standards and aspirations associated to non-digital processing across its services and processes so that customer journeys can be completed with minimal customer and operational effort

3. As the NS&I Business Owner, I want the supplier to provide a complaints management service in accordance with regulatory standards, so that we can ensure customers get the service they expect, and any failures in services are remediated

What's the business need?

- Improved customer experience through prompt assessment, investigation and resolution of complaints sent to NS&I by customers via any channel.
- Ensure regulatory compliance through tracking responsiveness against regulatory guidelines
- Prevent and/or minimise reputational damage through effective management of complex complaints
- Data and insight to support proactive root cause analysis in order to mitigate future issues.

Who will use these capabilities?

- Customer Contact Centre Agents
- The Director
- Customers

How will this be delivered?

The supplier will provide the resources, workforce, systems, processes, and training needed to deliver the required services in collaboration with NS&I and other Suppliers.

Scope of this requirement

The supplier will respond to complaints from customers that cannot be resolved at the initial point of contact. The supplier is expected to provide a fully integrated complaints management system and the IT capabilities for managing complaints.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-CMP-001	**Complaints Management**	The supplier shall record and resolve complaints in a timely manner In-line with agreed complaints framework adhering to FCA requirements, so that customer experience is improved.
PPCL2-CMP-002	**Complaints Management**	The supplier shall provide the capability to identify and register complaints received at first points of contact with all digital and non-digital channels including but not limited postal, telephone, social media etc. so that complaints are recognised and dealt with in a timely manner.

PPCL2-CMP-003	**Complaints Management**	The supplier shall design and deliver a defined complaints escalation process which is clear to the complaints operations team to follow so that they can effectively escalate complaints to the appropriate channels.
PPCL2-CMP-004	**Complaints Management**	The supplier shall deliver a complaint management service that supports effective ownership of reported issues so that actions are taken to rectify them within timelines agreed with the Director.
PPCL2-CMP-005	**Complaints Management**	The supplier shall deliver a process to support the Director to review and respond to specialist complaints including but not limited to HMT complaints, media complaints and MP complaints so that these high-profile complaints can be managed appropriately.
PPCL2-CMP-006	**Complaints Management**	The supplier shall deliver a complaint management service that supports cross system alignment of customer details so that customer information is kept up to date across the service and with other suppliers' systems.
PPCL2-CMP-007	**Complaints Management**	The supplier shall ensure customer data is accessible in one place so that complaints operations team can easily view customer information and business correspondence.
PPCL2-CMP-008	**Complaints Management**	The supplier shall design and employ appropriate methods to manage policy/large incident related complaints, so that they can be dealt with efficiently and consistently.
PPCL2-CMP-009	**Complaints Management**	The supplier shall ensure compensation is awarded to customers in line with compensation policy so that the complaint is resolved appropriately.
PPCL2-CMP-010	**Complaints Management**	The supplier shall capture and monitor root causes of complaints in order to generate actionable insights and recommendations so that appropriate remediation can applied to improve customer experience.
PPCL2-CMP-011	**Complaints Management**	The supplier will produce FCA reporting in line with FCA requirements for the Director to approve prior to issuance and publication so that the Director can review, input, and remain compliant with complaints reporting.
PPCL2-CMP-012	**Complaints Management**	The supplier shall collaborate with the Director to manage all FOS related queries so that oversight can be given to ensure all tasks are actioned.

PPCL2-CMP-013	**Complaints Management**	The supplier shall utilise complaints analysis to provide feedback and recommendations to specific business areas and staff in order, so that reoccurrence is reduced, and the service or process is continually improved.
PPCL2-CMP-014	**Complaints Management**	The supplier shall design and provide an effective data protection complaints management procedure, including specialists' knowledge and training for staff and agreed timelines for resolution, so that the Director remains in compliance with the relevant legislation.

4. As the NS&I Business Owner, I want the supplier to provide a document production and management service, so that NS&I can meet its accessibility obligations relating to customers unable to digitally self-serve

What's the business need?

- To produce, store, retrieve and where applicable destroy documents securely
- To effectively communicate with customers unable to digital self-serve in the most reliable and cost-efficient manner
- To receive post in scanning

Who will use these capabilities?

- Contact Centre Agents
- Back Office Teams
- Other Suppliers (PPB, PPD)

How will this be delivered?

The supplier will provide the resources, systems, processes and training needed to develop the required services in collaboration with NS&I and other Suppliers. Where necessary the supplier will implement and maintain the required system integrations across the technology landscape.

Scope of this requirement

- Document Management – storage, versioning, metadata, security, indexing and retrieval of digital documents
- Data collection - raw transactional data, scanned image data & OCR data
- Template Management and Approval
- Print document composition
- Integration capabilities to provide document management functionality directly to other applications.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-DPM-001	**Document Management**	The supplier shall provide a secure document storage and retrieval solution, so that documents received or issued can be stored and retained in line with the relevant regulatory (FCA), legal (data retention) and internal policies.
PPCL2-DPM-002	**Document Management**	The supplier shall digitise (e.g., scanning and OCR) inbound physical documentation received from customers so that requests for service can be efficiently provided via digital or automated means
PPCL2-DPM-003	**Document Management**	The supplier shall provide the capability to ingest, search, serve, modify, and deploy different file types so that the Director can utilise files in alignment with defined processes and procedures.
PPCL2-DPM-004	**Document Management**	The supplier shall process inbound/outbound post to the agreed level of requirements (e.g., postal classification, security, secure storage, retention etc.), so that customer experience, operational processing and record keeping can be delivered to agreed standard.
PPCL2-DPM-005	**Document Management**	The supplier shall manage (e.g., identify, scan, categorise etc.) inbound paper documents and route them to the appropriate workflow for processing, so that customer experience, operational processing and record keeping can be delivered to agreed standard.
PPCL2-DPM-006	**Document Management**	The supplier shall produce customer correspondence in paper or electronic format (including secure messages) by using pre-agreed letters and/or component paragraphs, including but not limited to; templates, forms, brochures, so that the supplier can communicate with customers within parameters agreed with the Director.
PPCL2-DPM-007	**Document Management**	The supplier shall ensure that the document management solution integrates with other services, so that information and data is available to support the construction of correspondence and delivery of relevant processes across the enterprise.
PPCL2-DPM-008	**Document Management**	The supplier shall provide scalable printing capabilities for the various types and volumes of required outputs, so that the Director can correspond with customers in a timely manner.

PPCL2-DPM-009	**Document Management**	The supplier shall provide the capability to print, control and dispatch warrants with the appropriate security measures, so that customers who are unable to receive electronic payment can receive accurate payment from the director in timely manner.
PPCL2-DPM-010	**Document Management**	The supplier shall provide a template storage and management solution, so that documentation formats can be standardised, reviewed, amended, and approved.
PPCL2-DPM-011	**Document Management**	The supplier shall deliver efficient, flexible, comprehensive testing and evidence of all electronic and printed documents newly specified by the Director and provide these to the Director for approval so that final output can be assured as correct.
PPCL2-DPM-012	**Document Management**	The supplier shall manage the end-to-end processing of cheques including banking, scanning, reconciliation, returning and post processing (destroy, return to customer, or retain in line with agreed retention policy) so that, customer payments and the Director's banking activities is appropriately operated and controlled.
PPCL2-DPM-013	**Document Management**	The supplier shall ensure that structured, semi-structured data and metadata is available to be used within the Insights capability, so that the Director is able to make effective operational and customer decisions.
PPCL2-DPM-014	**Document Management**	The supplier shall enable for stored data/correspondence to be linked to a customer record so that the Director and its suppliers have a full view of the customer and history of customer's interactions with the Director.

5. As the NS&I Business Owner, I want the supplier to provide any non-digital Prize Draw related operational processing, so that all prizes are allocated, exceptions resolved, and customers notified

What's the business need?

- To reduce costs and labour-intensive processes
- Improve customer experience through reduced processing times

Who will use these capabilities?

- Contact Centre Agents
- The Director
- Customers
- Other Suppliers (PPB, PPD)
- Back Office Teams

How will this be delivered?

The supplier will provide the resources, systems, processes, and training needed to develop the required services in collaboration with NS&I and other Suppliers. Where necessary the supplier will implement and maintain the required system integrations across the technology landscape.

Assumption: We assume that PPD supplier will be responsible for the provision, operation, execution and gaining the regular validation of the actual Prize Draw and core related systems, such as the random number generator and the "Prize Draw System" (PDS) and the Core Banking system.

Scope of this requirement

The operation of non-digitised Prize Draw processes that are not provided through Prize Draw System, including prize checking services, supporting the jackpot payment and those that cannot be automated.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-PD-001	**Non-Digital Prize Draw**	The supplier shall operate and support the elements of the Jackpot (£1m) winner services including preparation of specialist documentation and payment arrangements so that the winner has the positive customer experience.
PPCL2-PD-002	**Non-Digital Prize Draw**	The supplier shall accurately execute operational processing of customer journeys related to the Prize Draw, which cannot be completed with the digital processes, within appropriate timelines so that customers are provided with positive engagement experience.

		These services should include but not limited to Missed opportunities, Reserve prizes and Excess refund processing.
PPCL2-PD-003	**Non-Digital Prize Draw**	The supplier shall be able be make any permitted updates to the customer records as part of their interactions with the customers in the prize draw process / operations so that the accurate customer data is available and drives appropriate processes/adjustment in the Prize Draw process.
PPCL2-PD-004	**Non-Digital Prize Draw**	The supplier shall collaborate with NS&I and other suppliers to ensure that all suppliers meet their specific responsibilities in conducting the prize draw successfully.

6. As the NS&I Business Owner, I want the supplier to operate its defined and agreed customer services in accordance with all relevant risk frameworks and compliance legislation, so that NS&I delivers a trustworthy and safe customer experience

What's the need?

As a government agency, NS&I is subject to specific legislation. In addition, though not regulated as a bank, it operates in the UK's regulated retail banking market and applies a shadow compliance approach.

Who will use these capabilities?

NS&I's Risk and Compliance teams define the Compliance Universe and Risk Frameworks within which NS&I operates and assure compliance with those principles. The supplier will ensure that the principles are applied by design and through the development and improvement lifecycles.

How will this be delivered?

People engaged in delivering change will ensure that Compliance and Risk subject matter experts are organically involved in the design, development, and improvement processes.

Scope of this requirement

This requirement will ensure that operations are Compliant and operate within the Risk Framework for the span of the contract, from requirements analysis, through implementation and through ongoing BAU delivery and improvement.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPBL2-RC-001	**Risk**	The supplier shall operate a risk framework which meets the Government standard set out in the Orange Book and aligns as far as practicable with the Director's risk framework, so that the Director has assurance of risks being appropriately managed.
PPBL2-RC-002	**Risk**	The supplier shall provide real time access for the Director to comprehensive risk data, so that the Director has an accurate view of risk exposures.
PPBL2-RC-003	**Risk**	The supplier shall support any audit or assurance activities instigated by the Director both in the supplier operation and any approved subcontracting of services, so that the Director can be assured that work is being conducted to a high standard and in accordance with agreed contracts.
PPBL2-RC-004	**Compliance**	The supplier shall operate in compliance with the legislation relevant to the Director's business/operation, including, but not limited to, new, amended or extended legislation and any FCA requirements as would be required by a fully regulated deposit-taker, including the treatment of vulnerable customers and the handling of customer complaints, so that the Director can be assured that his legal and regulatory equivalence obligations are met, and the risks associated with those obligations are managed appropriately.
PPBL2-RC-005	**Compliance**	The supplier shall ensure that their staff, and the staff of their sub-contractors, where applicable, operate and conduct themselves in a way that is compliant with financial services industry requirements so that the Director can be assured that those staff are aware of their legal and regulatory obligations when working in the financial services sector, and conduct themselves accordingly.
PPBL2-RC-006	**Compliance**	The supplier shall ensure that any data is captured, processed, hosted and stored in accordance with relevant data protection legislation and the Director's customer data retention rules.

7. As the NS&I Business Owner, I want the supplier to work with the NS&I SIAM function and other suppliers to deliver our services, so that customers journeys are seamless across the multi-supplier model

What's the need?

This requirement provides the service management and integration framework to assure that the agreed service levels are met for: availability and performance of NS&I's customer contact and back-office operation; incident management and response; and infrastructure maintenance

Developing an always on, continuous improvement approach to business operations, incident resolution, and service integrations.

Who will use these capabilities?

NS&I has already carried out a procurement to provide Enterprise Architecture support for transforming NS&I's business, building internal capability, and creating a sustainable platform for delivery in the future. Further opportunities have also been identified for scaling internal capability in key areas, including service integration and management capability.

How will this be delivered?

The supplier will provide the resources, systems and processes need to interface with NS&I's SIAM function, and to implement and maintain the required system integrations.

Scope of this requirement

The supplier will need to embed with the new NS&I SIAM function and other suppliers to;

- Develop NS&I services,
- Develop NS&Is continuous improvement approach
- Develop NS&Is incident resolution and;
- Develop Service integration

Stakeholder requirements

Requirement ID	Grouping	Requirement description
PPCL2-SIM-001	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the Availability Management Policies and Procedures so that SIAM can ensure that the availability levels for all services comply with or exceed the agreed requirements in a cost-effective manner
PPCL2-SIM-002	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the Capacity Management Policies and Procedures so that SIAM can ensure that appropriate levels of resources and

		system performance are set and delivered, meeting the needs of the Director
PPCL2-SIM-003	**SIAM**	The Supplier shall monitor all events that occur, notifying the Director's SIAM function when it becomes aware of a potential Service Impacting Event so that exceptional conditions can be detected and escalated appropriately
PPCL2-SIM-004	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the IT Service Continuity Management Policies and Procedures so that emerging ITSCM risks or threats are mitigated to support business continuity
PPCL2-SIM-005	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the Service Asset and Configuration Management Policies and Procedures so that accurate asset and configuration data is maintained
PPCL2-SIM-006	**SIAM**	The Supplier shall provide all relevant information, including the detail, status, possible interactions and mutual dependencies, of all current services and those under development so that the Director's SIAM function is informed in the development, maintenance and distribution of the service catalogue
PPCL2-SIM-007	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the Service Level Management Policies and Procedures so that accurate service level management information and appropriate supporting documentation is provided
PPCL2-SIM-008	**SIAM**	The Supplier shall adhere to the Director's SIAM function policies and procedures that define standards and architecture so that operational standards and criteria are consistent and adhered to, providing an effective reference point for implementing and transitioning services
PPCL2-SIM-009	**SIAM**	The Supplier shall provide the Director's SIAM function with a feed of information according to the Financial Management Policies and Procedures so that the consumption of chargeable resources, catalogue requests and other change requests service charges can be validated
PPCL2-SIM-010	**SIAM**	The Supplier shall deliver services which are compliant with agreed service management policies, procedures and processes so that there is a consistent quality of service provision

PPCL2-SIM-011	**SIAM**	The Supplier shall identify named individuals to act as client relationship managers so that interfaces into the SIAM function and the Directors core functions are as seamless as possible
PPCL2-SIM-012	**SIAM**	The Supplier shall support the Director's SIAM function Service Desk by ensuring all relevant information is provided when contacts are made so that the service desk can deliver efficiently and maintain good management of the case
PPCL2-SIM-013	**SIAM**	The Supplier shall provide an effective data integration with the Director's SIAM function service desk tool(s) to facilitate incident management so that service availability, incident severity and resolution time metrics are met
PPCL2-SIM-014	**SIAM**	The Supplier shall support the Director's SIAM function with defining and executing the Service Request Management Policies and Procedures so that service requests are accurately captured, assigned and fulfilled
PPCL2-SIM-015	**SIAM**	The Supplier shall cooperate with the Director's SIAM function and other service providers on problem investigations so that problems are correctly identified and escalated
PPCL2-SIM-016	**SIAM**	The Supplier shall adhere to access management policies and procedures set by the Director's SIAM and/or security functions so that access to data and functionality is controlled appropriately.
PPCL2-SIM-017	**SIAM**	The Supplier shall ensure that all relevant service management information is made available to the Director's SIAM function so that the development of the service knowledge management repository is comprehensive
PPCL2-SIM-018	**SIAM**	The Supplier shall support the Director and its SIAM function with the service level design review so that the definition of the service levels, service targets and KPIs are clear and periodic audit reviews can take place
PPCL2-SIM-019	**SIAM**	The Supplier shall comply with the Service Management Policies and Procedures, including regulatory obligations, required by the Director's SIAM function and ensure that any non-compliance is raised and managed through to resolution
PPCL2-SIM-020	**SIAM**	The Supplier shall collaborate with the Director's SIAM function and other Suppliers to support Service Transition activities, so that they are aware of and

		approve their specific responsibilities of activity needed to deliver the transition or change successfully Service Transition activities include but are not limited to: service transition planning, integration testing and service evaluation.
PPCL2-SIM-021	**SIAM**	The Supplier shall assist the Director's SIAM function in the definition and execution of Change Management Policies and Procedures so that change is monitored and managed efficiently between Suppliers and the Director, reducing negative impacts
PPCL2-SIM-022	**SIAM**	The Supplier shall participate in scheduling releases with the Director's SIAM function and other service providers so that all Suppliers are informed of the plan allowing deployments to run smoothly
PPCL2-SIM-023	**SIAM**	The Supplier shall provide enhanced support post-deployment so that operations after new or changed services are smoothly delivered, ensuring swift remediation of issues
PPCL2-SIM-024	**SIAM**	The Supplier shall support the Director's SIAM function and other service providers with integration testing with so that testing is effective and ensures that all the service providers' components are integrated to provide the Director with stable, maintainable end-to-end service
PPCL2-SIM-025	**SIAM**	The Supplier shall provide future project activity information so that the Director's SIAM function can assess and schedule future test environment availability
PPCL2-SIM-026	**SIAM**	The Supplier shall liaise with the Director's SIAM function to align project portfolio and services to enterprise strategy, risk and security requirements and ensure outcomes delivered by multiple suppliers so that services are coherent and end-to-end
PPCL2-SIM-027	**SIAM**	The Supplier shall integrate and contribute to the Directors mandated knowledge management and collaboration tooling so that a central repository of corporate information is maintained
PPCL2-SIM-028	**SIAM**	The Supplier shall ensure that they have a comprehensive business continuity, Disaster recovery and Backup strategy and plan so that the Director's services are able to tolerate and recover from major events

PPCL2-SIM-029	**SIAM**	The Supplier shall contribute to an end-to-end Service Transition Approach and detailed plan so that there is evidence of their approach and activities required to transition services to its target state. Transition approach must be low risk, smooth, successful and have minimal impact on customers and the Director.
PPCL2-SIM-030	**SIAM**	The Supplier shall align with the cross-supplier collaborative ways of working so that the Director and its suppliers can work efficiently to achieve their common aims
PPCL2-SIM-031	**SIAM**	The Supplier shall support the Director in delivering insight-driven continuous improvement and delivery so that the Director can improve services frequently, iteratively and cost-effectively
PPCL2-SIM-032	**SIAM**	The Supplier shall ensure delivery and continuous improvements are driven by actionable insight into business drivers, end-to-end service needs, and operational performance so that the Director reduces the risk and maximises the effectiveness of service
PPCL2-SIM-033	**SIAM**	The Supplier shall operate with appropriate levels of devolved authority so that teams are self-sufficient and empowered to act on insight and can prioritise their deliverables
PPCL2-SIM-034	**SIAM**	The Supplier shall communicate with the Director and its Suppliers, sharing knowledge openly and transparently so that teams are empowered and have the information they need to make decisions
PPCL2-SIM-035	**SIAM**	The Supplier shall align with the Director's service governance so that the accountabilities and responsibilities for change and its risks, are clearly defined, understood, and managed
PPCL2-SIM-036	**SIAM**	The Supplier shall align with the Director's cadence of delivery so that management and delivery of service is coordinated across Suppliers, vendors, release paths, and touchpoints
PPCL2-SIM-037	**SIAM**	The Supplier shall leverage competitor and market intelligence so that the Director can maintain its fast follower status so that it refreshes its capabilities in line with emerging hygiene factors and best practice for procured services
PPCL2-SIM-038	**SIAM**	The Supplier shall provide end-to-end reporting and monitoring capabilities, so that the Director has oversight over operations and security of the solution

8. As the NS&I Business Owner, I want the supplier to operate in a manner which protects NS&I customers from security threats and attacks, so that NS&I's brand and reputation are maintained

What's the business need?

- To protect NS&I's customers, brand, and activities, ensuring that digital and non-digital touch points are appropriately secures.
- To ensure that contact centre and back-office processing are secure so that NS&I's customers and prospective customers are assured of their transactions and information are safe.

Who will use these capabilities?

The supplier will follow best-practice security guidelines throughout the lifecycle of implementation and ongoing continuous improvement. Thy will provide the information needed to prove security of activities being undertaken and so that attacks can be detected and responded to in a timely manner. NS&I's Security function will conduct assurance that sufficient and adequate security measures are being implemented and will coordinate cross-supplier incident management.

How will this be delivered?

The supplier will follow good security practice during design and implementation so that deployments or any significant changes are done securely and do not pose a security threat to NS&I's wider ecosystem. They will ensure that customers are protected against fraud and have appropriate access to services with as little friction as possible.

Scope of this requirement

This requirement extends to the capabilities delivered by this package, and the to the services delivered to customers that are enabled by those capabilities.

Stakeholder requirements

Requirement ID	Grouping	Requirement description
PPCL2-SEC-001	**Security**	The Supplier shall follow good security practice during implementation and throughout the life of the contract to enable business operations to be conducted in a secure manner and in line with the Directors requirements and standards.
PPCL2-SEC-002	**Security**	The Supplier shall ensure that all of the Director's services across all channels are secured in line with the Directors requirements and standards.
PPCL2-SEC-003	**Security**	The Supplier shall ensure the customer and user access to the systems and applications is

		authenticated and authorised so that the Director can maintain confidentiality, integrity and availability.
PPCL2-SEC-004	**Security**	The Supplier shall ensure that information is exchanged securely with other services and organisations, so that the confidentiality, integrity and availability of the solution and its information is protected at all times.
PPCL2-SEC-005	**Security**	The Supplier shall implement measures to protect the Director's brand and activities so that customers are reassured that they are safe, and their information is secure when accessing the Director's contact centre support services.
PPCL2-SEC-006	**Security**	The Supplier shall provide logs and event data to the Director's security monitoring solution so that attacks can be detected and responded to in a timely manner.
PPCL2-SEC-007	**Security**	The Supplier shall ensure design and development activities are undertaken securely so that deployments or any significant changes are done securely and do not pose a security threat to the Director's wider ecosystem.
PPCL2-SEC-008	**Security**	The Supplier shall be willing to provide the information needed to the Director to prove security of activities being undertaken, so that the Director has adequate assurance that sufficient and adequate security measures are being implemented.
PPCL2-SEC-009	**Security**	The Supplier shall design and implement a business continuity management system (BCMS) certified independently to ISO22301 standards which covers the scope of all services provided and is accepted by the director, so that the business can recover in the event of an incident.
PPCL2-SEC-010	**Security**	The Supplier shall collect, maintain, store and deliver all information in compliance with Information Management principles so that information is available to the right people at the right time.

9. As the NS&I Business Owner, I want the supplier to develop and operate its services in accordance with NS&I architectural design standards, including utilisation of any prescribed technologies, so that NS&I remains architecturally coherent, and services can easily be re-procured in the future

What's the need?

NS&I has defined architectural and design principles, which are governed by the Enterprise Architecture function. These principles assure compatibility of each package with the overall architecture design, and with overarching frameworks such as UK Government's Technology Code of Practice.

Who will use these capabilities?

NS&I will use the outcomes from this requirement to assure the supplier activities and ongoing deliverables comply with.

- The Enterprise Architecture requirements and design principles
- The technical and non-technical design, development, testing, and release lifecycle methodology and requirements.

How will this be delivered?

Through compliance with NS&I's Enterprise Architecture processes and governance, and delivery of agreed design, development, and process artefacts.

Scope of this requirement

The supplier will need to:

- comply and align with NS&I's architecture design standards, governance and enterprise architecture frameworks
- use enterprise-wide technologies and standards so as to enable system integration and maintain design cohesion
- assure that services will be available to be re-procured in the future
- align in quality assurance, including any testing and transition requirements

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-ART-001	**Architecture Design Standards**	The Supplier shall design, build and operate the procured solutions in collaboration with other Supplier solutions by participating in the Director's Design Governance Processes. This shall be done across the Transition States and beyond, so that seamless end-to-end services are delivered.

PPCL2-ART-002	**Architecture Design Standards**	The Supplier shall make available to the Director resources and documentation relevant to its intellectual property, so that the Director has access to information required to run and maintain the solution being procured. Information and documentation include but is not limited to: configurations used, code repository, design documentation, escrow arrangements
PPCL2-ART-003	**Architecture Design Standards**	The Supplier shall design solutions in accordance with the Directors architectural standards and principles so that the Director enterprise architecture has design coherence
PPCL2-ART-004	**Architecture Design Standards**	The Supplier shall utilise the Directors prescribed technologies, where appropriate, so that the Director can have an integrated estate of services
PPCL2-ART-005	**Architecture Design Standards**	The Supplier shall design, build and operate the procured solutions in collaboration with other Supplier solutions so that seamless end-to-end services are delivered.
PPCL2-ART-006	**Architecture Design Standards**	The Supplier shall provide resilient solutions so that services to the Director's customers are available as much as possible
PPCL2-ART-007	**Architecture Design Standards**	The Supplier shall comply with the non-functional characteristics of the Directors requirements so that the services meet the business needs
PPCL2-ART-008	**Architecture Design Standards**	The Supplier shall provide all infrastructure and development environments required (hardware and software), so that the platform is not reliant on the Director's provided infrastructure.
PPCL2-ART-009	**Architecture Design Standards**	The Supplier shall provide change management capabilities so that the customer and business outcomes from the solution are continuously improved.
PPCL2-ART-010	**Architecture Design Standards**	The Supplier shall ensure that each element of their solution is designed & tested for accessibility, so that staff are able to complete their "Jobs to be done".
PPCL2-ART-011	**Architecture Design Standards**	The Solution shall provide employee identity and access management capabilities, so that the Director's staff access is controlled and regulated as required.

PPCL2-ART-012	**Architecture Design Standards**	The Supplier shall work collaboratively with other Suppliers to carry out and support migration activities, so that any required data and/or system migrations can be carried out in a reliable and efficient manner.
PPCL2-ART-013	**Architecture Design Standards**	The Solution shall provide monitoring capabilities, so that the Director has oversight over operations and security of the solution.
PPCL2-ART-014	**Architecture Design Standards**	The Supplier shall provide insights into how they are developing their product roadmap, so that the Director can be assured that the product suite is being actively developed and that the roadmap aligns with the Director's strategic vision.
PPCL2-ART-015	**Architecture Design Standards**	The Supplier shall continuously share with the Director any expected changes to roadmaps, so that the Director can perform the required market/competitor analysis before any products are developed and are aware of any upcoming changes which can be in turn prioritised.
PPCL2-ART-016	**Architecture Design Standards**	The Supplier's solution shall enable intelligence from individual capabilities to be combined with data and intelligence from other areas of the business, so that it can be analysed for reporting and to develop new insights which inform recommendations for improving the customer experience.
PPCL2-ART-017	**Architecture Design Standards**	The Supplier's solution shall provide actionable insight into operation and service issues, so that the Director is able to understand what the problems are and what to do about them.
PPCL2-ART-018	**Architecture Design Standards**	The Supplier's solution shall deliver actionable insight to the right destination and at the right frequency, so that the Director and its Suppliers can meet the agreed cadence of continuous development and improvement.
PPCL2-ART-019	**Architecture Design Standards**	The Supplier shall maintain versions of Solution’s components and services at mainstream supported levels, so that the Director has minimised security and design flaw exposure
PPCL2-ART-020	**Architecture Design Standards**	The Supplier shall ensure the accuracy and integrity of all data within their provisioned services, so that the customer and operational journey remains positive, and the Director fulfils its HM Treasury requirements
PPCL2-ART-021	**Architecture Design Standards**	The Supplier shall collaborate with other Suppliers and the Director to ensure the end-to-end data consistency and integrity, so that the Director can deliver seamless end-to-end services

10. As the NS&I Business Owner, I want the supplier to provide NS&I with relevant competitor, service, and customer intelligence, so that NS&I can continuously improve its propositions and services

What's the business need?

This package will introduce new ways of working that use actionable insight into customer needs and behaviour to drive frequent, rapid, and iterative deliveries of business and customer value. Those ways of working will leverage new capabilities and use customer data to tailor and personalise experiences in alignment with NS&I's Customer Experience Framework, and to meet the needs of target customers to achieve their Jobs to be Done, as defined in the Customer Value Propositions.

Who will use these capabilities?

NS&I Operations and Assurance teams.

How will this be delivered?

Suppliers will be required to collect data, analyse it, and collate it into actionable insight. This should be delivered to the right stakeholders at an agreed pace to ensure we can maintain the desired cadence of delivery.

The requirement will also provide near real-time data for operational performance monitoring, incident, and complaints management.

Scope of this requirement

NS&I has existing capabilities for delivering the types of intelligence in scope of these requirements. Within the scope of this package, we will look at how we supplement these with new supplier capabilities. The NS&I and supplier roles will cover different levels of insight:

- NS&I - from strategy down. NS&I's role, market position, business performance, product offer, and customer offer
- Suppliers - closing the feedback loop from service delivery to customer response. Focused on customer touchpoints, interactions, journeys, and experiences.

Within the supplier domain, we will require these kinds of actionable insight.

- Competitor - what can we learn from best market practice, particularly from what suppliers have done for other clients, as applied to the below
- Service - what are the pain points and causes of friction, what causes them, and how do we fix them
- Customer - how are customers responding to our services, and how does this impact on key metrics (e.g., trust, CSAT).

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure access to, creation and amendment of the appropriate customer data, so that the Director can provide the required tailored service to all customers, as needed
PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier's solution shall integrate data and insight with other parts of the wider Directors ecosystem, so that the Director can ensure delivery and continuous improvement of all its services
PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier's solution shall provide actionable insight regarding customer experience and operations of the service, to a cadence agreed with the Director, so that the Director and other Suppliers are able to understand the underlying cause of issues and continuously improve
PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The supplier's solution shall enable access to operational data, so that the Director and its suppliers can assess and improve operational effectiveness of services provided within the procurement package.
PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall provide customer journey recommendations for all Supplier provisioned services, so that the Directors customer experience can be continuously improved across all services
PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The supplier shall create and manage data according to the Director's Data Governance standards, processes and forums so that the provisioned data and any actionable insight can be relied upon by the Directors organisation

11. As the NS&I Business Owner, I want the supplier to promote adoption of digital services so that NS&I can move from current to future operating model

What's the business need?

- To automate where possible manual processes
- To promote highly digitized straight-through customer experiences
- To encourage existing customers to convert to paperless digitized journeys

Who will use these capabilities?

- Contact Centre Agents
- Customers
- Back Office Teams
-

How will this be delivered?

The supplier will provide the resources, systems, processes and training needed to develop the required services in collaboration with NS&I and other Suppliers.

Scope of this requirement

The scope will cover the end to end support of the transformation to a new operating model and ways of working.

Stakeholder requirements

Requirement ID	Grouping	Requirement description
PPCL2-TRF-001	**Transformation**	The supplier shall deliver, for Director agreement, and then execute against a strategy to appropriately drive customers to use the digital self serve-service, so that the Director can be assured of a strategy and delivery against that strategy, that achieves a transformational move to digital customer self service during the contract period, whilst always ensuring suitable customer outcomes.

12. As the NS&I Business Owner, I want the supplier to provide financial crime investigation and management services, so that NS&I can meet obligations to protect its customers and minimise losses through criminal activity

What's the need?

For NS&I to protect itself and its customers by providing Financial Crime investigation and management services. In addition to ensuring all staff are fully trained to detect and take action on potential suspicious activity, investigate and report on potential fraudulent activity, and manage relationships with customers identified as high-risk for money laundering, etc

Who will use these capabilities?

NS&I Contact Centre agents, NS&I's Financial Crime Team, NS&I PPC staff, and other suppliers**.**

How will this be delivered?

The supplier will provide resources, systems, people and processes, and training needed to develop the required services in collaboration with NS&I and other Suppliers. The supplier will need to include a solution to receive alerts from across NS&I and track their investigations to closure.

Scope of this requirement

The requirements are for the span of the contract, from requirements analysis, through implementation and ongoing BAU delivery and improvement. In addition, will also cover the investigation of all aspects of potential financial crime activity, as well as the identification of suspicious activity within the general scope of the PPC service.

Stakeholder requirements (UPDATED – see section 5 for details)

Requirement ID	Grouping	Requirement description
PPCL2-FC-001	**Financial Crime**	The Supplier shall act where customers are matched against lists and feeds to validate the match and identify appropriate actions agreed with the Director so that risky customer relationships and actions for ongoing due diligence can be identified
PPCL2-FC-002	**Financial Crime**	The Supplier shall appropriately manage the ongoing due diligence of NS&I customers to validate and investigate these, and take appropriate actions, so that financial crime risks are managed within agreed tolerances
PPCL2-FC-003	**Financial Crime**	The Supplier shall identify potentially suspicious behaviour in customer interactions with the contact centre so that effective risk management controls are applied
PPCL2-FC-004	**Financial Crime**	The Supplier shall provide the ability to manage financial crime cases and investigations so that the Director minimises reputational damage and financial losses and the Director maintains legal compliance
PPCL2-FC-005	**Financial Crime**	The Supplier shall ensure and evidence the appropriate oversight of setting and maintenance of business rules, controls and configuration changes so that they are aligning to the Directors risk appetite and policies
PPCL2-FC-006	**Financial Crime**	The Supplier shall assure that business rules, controls and configuration changes are defined and implemented so that they are aligning to the Directors risk appetite and policies
PPCL2-FC-007	**Financial Crime**	The Supplier shall make risk-based decisions based on recent customer behaviour for the purposes of requiring enhanced customer authentication, informed by the full Directors data set so that account information is not handed to bad actors.
PPCL2-FC-008	**Financial Crime**	The Supplier shall have controls in place to identify unauthorised insider access to or activity on customer accounts, and if any suspicious activity is defined, it is investigated with the finding reported to the Director, to ensure customer accounts are safeguarded.

PPCL2-FC-009	**Financial Crime**	The supplier shall ensure appropriate staffing levels are in place to discharge the services of the Financial Crime function. Staff operational hours are to be agreed with the Director.
PPCL2-FC-010	**Financial Crime**	The supplier shall ensure the outsourced financial crime function is designed and operates in line with guidance from the UK's Joint Money Laundering Steering Group and the FCA Financial Crime Guide: A firm's guide to countering financial crime risks. The supplier shall ensure any future revisions of such guidance are adhered to and applied to the outsourced NS&I Financial Crime Function.

5. Changes from the original version, and previous version issued.

Grouping	Requirement ID	Replaced Requirement	New Requirement ID	New Requirement (if applicable)
Assisted Digital	PPCL2-AD-010	The supplier shall provide a Co-Browsing capability to Director's apps and websites to facilitate Assisted Digital customer servicing.	Deleted (23/02/23)	
Non-Digital Prize Draw	PPCL2-PD-001	The supplier shall provide automated prize checker service for customers via phone so that the customers are able to check if they have been the prize winner or not.	Deleted	
Non-Digital Prize Draw	PPCL2-PD-004	The supplier shall provide operational processing related to Missed Opportunities in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	This is now a level 3 requirement under PPCL2-PD-002	
Non-Digital Prize Draw	PPCL2-PD-005	The supplier shall provide operational processing for the manual services related to Reserve Prizes in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys	This is now a level 3 requirement under PPCL2-PD-002	

		can be completed with minimal customer and operational effort.		
Non-Digital Prize Draw	PPCL2-PD-006	The supplier shall provide operational processing for the manual services related to Excess Refund Processing in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	This is now a level 3 requirement under PPCL2-PD-002	
Non-Digital Prize Draw	PPCL2-PD-009	The supplier shall collaborate with NS&I and other suppliers to support NS&I's automated and digital self-service activities so that NS&I can reduce risks and maximise the efficiency of the prize draw.	This is now a level 3 requirement under PPCL2-PD-004	
Competitor, Service and Customer Intelligence	PPCL2-INT-001	The supplier shall collect, maintain, store and deliver all information in compliance with Information Management principles so that information is available to the right people at the right time.	Deleted	
Competitor, Service and Customer Intelligence	PPCL2-INT-002	The supplier's solution shall enable the customer record to be populated with the data, attributes, permissions and customer preferences, so that the Director and its suppliers can tailor the content, experiences, and messages delivered to customers.	Deleted	
Competitor, Service and Customer Intelligence	PPCL2-INT-003	The Supplier's solution shall enable access to data, attributes, permissions in the customer record so that the Director and its suppliers can design, develop, and deliver tailored content,	PPCL2-INT-001	The Supplier shall ensure access to, creation and amendment of the appropriate customer data, so that the Director can

		experiences, and messages to customers and customer preferences.		provide the required tailored service to all customers, as needed
Competitor, Service and Customer Intelligence	PPCL2-INT-004	The supplier's solution shall integrate data from other parts of the wider Director ecosystem, so that combined data sources can be leveraged by the Director for tailoring/mass personalisation of communication regarding e.g. services and/or products.	PPCL2-INT-002	The Supplier's solution shall integrate data and insight with other parts of the wider Directors ecosystem, so that the Director can ensure delivery and continuous improvement of all its services
Competitor, Service and Customer Intelligence	PPCL2-INT-005	The supplier's solution shall enable customer, service and customer intelligence to be combined with data and intelligence from other areas of the business, so that it can be analysed for reporting and to develop new insights which inform recommendations for improving the end-to-end customer experience.	Deleted	
Competitor, Service and Customer Intelligence	PPCL2-INT-006	The supplier shall provide MI and actionable insights on how journeys perform across all the channels and recommendations so that assisted digital and non-digital routes can be improved for customer need, processing quality and efficiency. This MI should be easily accessible to the Director and other suppliers.	PPCL2-INT-003	The Supplier's solution shall provide actionable insight regarding customer experience and operations of the service, to a cadence agreed with the Director, so that the Director and other Suppliers are able to understand the underlying cause of issues and continuously improve
Competitor, Service and Customer Intelligence	PPCL2-INT-007	The supplier's solution shall deliver actionable insight to the right destination and at the right frequency, so that the Director and its suppliers can meet the agreed cadence of continuous development and improvement.	Deleted	
Competitor, Service and	PPCL2-INT-009	The supplier shall enable customers and other suppliers to capture and update data for inclusion	Deleted	

Customer Intelligence		into the customer record so that the Director can ensure accurate information is held on customers.		
Competitor, Service and Customer Intelligence	PPCL2-INT-010	The supplier shall provide MI and actionable insights on how journeys perform across all the channels and recommendations so that assisted digital and non-digital routes can be improved for customer need, processing quality and efficiency. This MI should be easily accessible to the Director and other suppliers.	PPCL2-INT-005	The Supplier shall provide customer journey recommendations for all Supplier provisioned services, so that the Directors customer experience can be continuously improved across all services
Competitor, Service and Customer Intelligence	PPCL2-INT-011	The supplier shall deliver a non-digital operations service with near/real time, automated Management Information capability including but not limited to real time workflow data/ queue monitoring/AI capabilities so that actionable insight and decision making is supported.	Deleted	
Competitor, Service and Customer Intelligence	PPCL2-INT-012	The supplier shall provide a workforce management tool to optimise workforce efficiency and increase productivity through relevant means such as workforce planning and forecasting, skills matrix development, robust analytics and AI with industry benchmarking so that workforce training and decision making is improved.	Deleted	
Competitor, Service and Customer Intelligence	PPCL2-INT-013	The supplier shall provide the Director access to its analytical tools so that the Director is able to combine insights about its operations and customers with other suppliers.	Deleted	
Architecture Design Standards	PPCL2-ART-012	The Supplier shall work collaboratively with other Suppliers to carry out and support migration activities, so that any required data and/or system	PPCL2-ART-012	The Supplier shall work collaboratively with other Suppliers to carry out and support migration activities, so that any required data migrations

		migrations can be carried out in a reliable and efficient manner.		can be carried out in a reliable and efficient manner.
Compliance	PPCL2-RC-004	The supplier shall operate in compliance with the legislation relevant to the Director's business/operation (as set out in the Compliance Universe document) so that the Director can be assured that his legal and regulatory obligations are met, and the risks associated with those obligations are managed appropriately	PPCL2-RC-004	The supplier shall operate in compliance with the legislation relevant to the Director's business/operation, including, but not limited to, new, amended or extended legislation and any FCA requirements as would be required by a fully regulated deposit-taker, including the treatment of vulnerable customers and the handling of customer complaints, so that the Director can be assured that his legal and regulatory equivalence obligations are met, and the risks associated with those obligations are managed appropriately.
Compliance	PPCL2-RC-007	The supplier shall supply a solution that enables the product to be serviced in compliance with the product terms and conditions and any applicable legislation.	Deleted	
Complaints Management	PPCL2-CMP-001	The supplier shall record and resolve complaints in a timely manner In-line with agreed complaints framework, so that customer experience is improved.	PPCL2-CMP-001	The supplier shall record and resolve complaints in a timely manner In-line with agreed complaints framework adhering to FCA requirements, so that customer experience is improved (Updated 23/02/23)
Complaints Management	PPCL2-CMP-010	The supplier shall capture and monitor root causes of complaints so that actionable insights and recommendations to improve customer experience can be effectively generate	Deleted	

Complaints Management	PPCL2-CMP-013	The supplier shall utilise complaints analysis to provide feedback and recommendations to specific business areas and staff in order so that reoccurrence is reduced, and the service or process is continually improved.	PPCL2-CMP-013	The supplier shall utilise complaints analysis to provide feedback and recommendations to specific business areas (across all suppliers) and staff in order so that reoccurrence is reduced, and the service or process is continually improved.
Complaints Management	PPCL2-CMP-016	The supplier shall deliver an effective and proactive root cause management and analysis capability for complaints so that trends can be easily identified and addressed to improve the service.	Deleted	
Document Management	PPCL2-DPM-003	The supplier shall provide the capability to ingest, store, search, serve, modify and deploy different file types so that the Director can utilise files in alignment with defined processes and procedures.	PPCL2-DPM-003	The supplier shall provide the capability to ingest, search, serve, modify and deploy different file types so that the Director can utilise files in alignment with defined processes and procedures.
Document Management	PPCL2-DPM-006	The supplier shall produce customer correspondence in paper or electronic format (including secure messages) by using pre-agreed letters and/or component paragraphs, including but not limited to; letters, forms, brochures, so that the supplier can communicate with customers within parameters agreed with the Director.	PPCL2-DPM-006	The supplier shall produce customer correspondence in paper or electronic format (including secure messages) by using pre-agreed templates and/or component paragraphs, including but not limited to; letters, forms, brochures, so that the supplier can communicate with customers within parameters agreed with the Director

Document Management	PPCL2-DPM-012	The supplier shall ensure adequate and secure record/document storage and efficient retrieval process is provided so that, documents received or issued can be securely stored and retained in line with the relevant regulatory (FCA), legal (data retention) and internal policies.	Deleted	
Document Management	PPCL2-DPM-014	The supplier shall provide the capability for physical documentation storage and digitisation, so that the Director is able to securely retain and optimise the processing of its records.	Deleted	
Non-Digital Operational Processing	PPCL2-OPS-020	The supplier shall identify and notify the Director of regulatory requests such as but not limited to FOI and Data Subject Rights requests so that the Director can meet its compliance and legal obligations within the agreed regulatory time frames.	Deleted	
Non – Digital Operational Processing	NEW		PPCL2-OPS-022	The supplier shall apply the following principles, standards and aspirations associated to non-digital processing across its services and processes so that customer journeys can be completed with minimal customer and operational effort
Financial Crime	PPCL2-FC-003	The Supplier shall identify potentially suspicious behaviour in customer interactions with the contact centre so that effective risk management controls are applied	PPCL2-FC-003	The Supplier shall identify potentially suspicious behaviour in customer interactions with the CIC so that effective safeguarding of customer and the Directors assets is ensured

Financial Crime	PPCL2-FC-009	The Supplier shall set risk tolerances for all capabilities in accordance with the Directors policies and risk tolerance so that there is a uniform approach to risk management across all areas	Deleted	
Financial Crime	PPCL2-FC-009	The Financial Crime service providers will operate between 7am - 7pm Mon - Fri (excluding Bank holidays) and the enabling solution capabilities will be available 24x7x365. Skeleton services will be provided by the Financial Services provider during the weekend (7am - 2pm)	PPCL2-FC-009	The supplier shall ensure appropriate staffing levels are in place to discharge the services of the Financial Crime function. Staff operational hours are to be agreed with the Director.
Financial Crime	New		PPCL2-FC-010	The supplier shall ensure the outsourced financial crime function is designed and operates in line with guidance from the UK's Joint Money Laundering Steering Group and the FCA Financial Crime Guide: A firm's guide to countering financial crime risks. The supplier shall ensure any future revisions of such guidance are adhered to and applied to the outsourced NS&I Financial Crime Function.
Security	PPCL2-SEC-010	The Supplier shall collect, maintain, store and deliver all information in compliance with Information Management principles so that information is available to the right people at the right time.	Merged as an L3	

Security	PPCL2-SEC-011	The solution shall provide employee identity and access management capabilities, so that the Director's staff access is controlled and regulated as required.	Merged as an L3	
Transformation	PPCL2-TRF-001	The supplier shall demonstrate how they will help to drive the customers to use the digital self serve-service, so that the Director has a clear understanding of the journey from current state to the future operating model.	PPCL2-TRF-001	The supplier shall deliver, for Director agreement, and then execute against a strategy to appropriately drive customers to use the digital self serve-service, so that the Director can be assured of a strategy and delivery against that strategy, that achieves a transformational move to digital customer self service during the contract period, whilst always ensuring suitable customer outcomes. (Updated 23/02/23)

6. Appendices

6.1 Detailed Level Three Requirements

The detailed level three requirements can be found in a separate document

PPC - Lot 2 - Volume 2 - Requirements Catalogue – V2.0

6.2 Requirements Glossary

This is a requirements glossary which incorporates IT, Procurement, Security, Data and Business glossary definitions. If there are any further definitions required contact the procurement team.

Data Definitions

#	Term	Description
DATA001	**Public**	Data that may be freely disclosed to the public
DATA002	**Internal-only**	Internal data not meant for public disclosure
DATA003	**Confidential**	Sensitive data that if compromised could negatively affect operations
DATA004	**Restricted**	Highly sensitive corporate data that if compromised could put the organisation at financial or legal risk

Security Definitions

#	Term	Description
SEC001	**Adaptive Authentication**	Multi-Factor Authentication that steps-up to additional factors based on configurable risk analysis of the user's behaviour and/or attributes
SEC002	**Anti-Malware Software**	A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.
SEC003	**Attacker**	Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.
SEC004	**Authentication Credentials**	A user's Authentication information used to reassert an established trust relationship. Typically consists of a user identifier and multiple factors from: Knowledge: something you know, eg a password Possession: something you have, eg a device Inherence: something you are, eg a biometric

SEC005	**Botnet**	A network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.
SEC006	**Breach**	An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.
SEC007	**Brute Force Attack**	Using a computational power to automatically enter a huge number of combination of values, usually in order to discover passwords and gain access.
SEC008	**Certificate**	A form of digital identity for a computer, user or organisation to allow the authentication and secure exchange of information.
SEC009	**CIAM**	Customer Identity Access Management. Facilities to ensure that customers identities are verified, authenticated on login and that the customer is granted access to the resources and services that they are entitled to, in a way that contributes to their user journey
SEC010	**Cyber Attack**	Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.
SEC011	**Cyber Essentials**	A cyber certification scheme operated by the National Cyber Security Centre
SEC012	**Cyber Incident**	A breach of the security rules for a system or service - most commonly; Attempts to gain unauthorised access to a system and/or to data.
SEC013	**Cyber Security**	The protection of devices, services and networks — and the information on them — from theft or damage.
SEC014	**Denial Of Service (DoS)**	When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.
SEC015	**Deny List**	An access control mechanism that blocks named entities from communicating with a computer, site or network. Can also be known as 'blacklisting' across the industry.
SEC016	**Dictionary Attack**	A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.
SEC017	**Digital Footprint**	A 'footprint' of digital information that a user's online activity leaves behind.
SEC018	**Download Attack**	The unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be known as a drive-by download.
SEC020	**Exploit**	May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.
SEC021	**Hacker**	In mainstream use as being someone with some computer skills who uses them to break into computers, systems and networks.

SEC022	**Honeypot (Honeynet)**	Decoy system or network to attract potential attackers that helps limit access to actual systems by detecting and deflecting or learning from an attack. Multiple honeypots form a honeynet.
SEC023	**Malvertising**	Using online advertising as a delivery method for malware.
SEC024	**Malware**	Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.
SEC025	**NIST CSF**	National Institute of Standards and Technology Cyber Security Framework – An internationally recognised standard framework for cyber security requirements.
SEC026	**Out-of-Band Authentication**	Authentication over a different Channel than the one on which the Customer is transacting. For example, if the Customer is transacting online, a one-time-passcode is sent via a push notification
SEC027	**Pen Test**	Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.
SEC028	**Personal Data**	shall have the same meaning as set out in the GDPR;
SEC029	**Personal Data Breach**	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Director Personal Data transmitted, stored or otherwise Processed;
SEC030	**Pharming**	An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.
SEC031	**Phishing**	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
SEC032	**Ransomware**	Malicious software that makes data or systems unusable until the victim makes a payment.
SEC033	**Sanitisation**	Using electronic or physical destruction methods to securely erase or remove data from memory.
SEC034	**Smishing**	Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.
SEC035	**Social Engineering**	Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.
SEC036	**Spear-Phishing**	A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

SEC037	**Strong Customer Authentication (SCA)**	Multi-Factor Authentication that complies with the Regulatory Technical Standard (RTS) of Payment Services Directive 2 (PSD2). The RTS applies only to Digital, not to phone interactions. It specifies stepping up to additional factors via Out of Band Authentication when - - Authenticating for the first time - Authenticating when 90 days has elapsed since the last step up - Viewing a transaction history dating back 90 or more days and when 90 days has elapsed since the last step up - Making a payment to or setting up a new trusted beneficiary (equivalent to an Director Nominated Account) The RTS does not preclude additional risk rules so long as they do not weaken the RTS prescriptions. For example, stepping up at every log-in is stronger than the RTS rules and may provide a better customer experience Additionally, the RTS specifies Dynamic Linking - when making a payment to a non-trusted beneficiary, Authentication notifications should include the beneficiary name, the payment amount, and a transaction reference. Note - Director terms do not permit payments to non-trusted beneficiaries
SEC038	**Threat**	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
SEC039	**Threat Actor**	An individual or a group posing a threat
SEC040	**Threat Intelligence**	Information about Threats that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
SEC041	**Trojan**	A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.
SEC042	**Two-Factor Authentication (2FA)**	Multi-Factor Authentication requiring only two factors
SEC043	**Virus**	Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.
SEC044	**Vulnerability**	A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

SEC045	**Water-Holing (Watering Hole Attack)**	Setting up a fake website (or compromising a real one) in order to exploit visiting users.
SEC046	**Whaling**	Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.
SEC047	**Zero-Day**	Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

Procurement Definitions

#	Term	Description
PROC001	**Advisers**	means all professional advisers of the Director involved in the procurement of the Project
PROC002	**Director**	means the Director of Savings, for National Savings & Investments, an Executive Agency of the Chancellor of the Exchequer whose office is at 1 Drummond Gate, London, SW1V 2QX
PROC003	**Award Criteria**	means criteria used by the Director to determine which of the Bids represents the most economically advantageous tender, in accordance with Regulation 67 of PCR 2015
PROC004	**Bid**	means each of the written proposals and any accompanying materials submitted by a Bidder as part of this procurement process at any stage of the procurement
PROC005	**Bidder**	means individuals and/or organisations who have been shortlisted at the selection stage, and to whom the ISIT has been issued by the Director
PROC006	**Candidate**	means individuals and/or organisations seeking to participate in this procurement process at the selection stage, but who have not been shortlisted and invited to the ISIT stage, either because the shortlisting stage has not yet concluded, or because the Candidate has been de-selected / disqualified

PROC007	**Confidential Information**	(a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Agreement that relates to: (i) the Disclosing Party Group; or (ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, know-how and/or personnel of the Disclosing Party Group; (b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Agreement that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Agreement; (c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Agreement and all matters arising therefrom; and (d) Information derived from any of the above, but not including any Information which: (i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party; (ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient; (iii) otherwise than by a breach of this Agreement or breach of a duty of confidentiality; (iv) was independently developed without access to the Confidential Information; or (v) relates to the Supplier's: (1) performance under this Agreement; or (2) failure to pay any Sub-contractor as required pursuant to Clause 15.15.1 (Supply Chain Protection).
PROC008	**Consortium**	means either an entity which is to be formed by a group of Organisations or a group of Organisations acting jointly as the Candidate or Bidder
PROC009	**Consortium Member**	means where the Candidate or Bidder is a Consortium, any individual economic operator forming part of that Consortium
PROC010	**Contract / Agreement**	means the contract between the Director and the successful Bidder to deliver the services in the Statement of Requirements, which are the subject of this procurement process
PROC011	**Contract Notice**	means the contract notice published in the FTS in respect of the Proposed Contract
PROC012	**CPN**	means the competitive procedure with negotiation as set out in Regulation 29 of the PCR 2015
PROC013	**EIR**	Means the Environmental Information Regulations 2004
PROC014	**Final Tender**	means the final tender Bids that Bidders will be required to submit in response to the Director's ISFT document

PROC015	**FTS**	means the Find A Tender UK e-notification service (within the meaning of the PCR 2015) where notices for new procurements are now required to be published in place of the Official Journal of the EU's Tenders Electronic Daily (OJEU/TED)
PROC016	**FOIA**	means the Freedom of Information Act 2000
PROC017	**Information Request**	means an information request under the FOIA or EIR
PROC018	**Initial Tender**	Means the initial tender Bids that Bidders will submit in response to the ISIT
PROC019	**ISIT**	means the Invitation to Submit Initial Tenders document that will be issued to shortlisted Bidders following the evaluation of SQ applications
PROC020	**ITN**	means the Invitation to Negotiate document that will be issued to shortlisted Bidders following the evaluation of Initial Tenders
PROC021	**ISFT**	means the Invitation to Submit Final Tenders that will be issued to the Bidders following the conclusion of the ITN negotiation stage
PROC022	**Marking Scheme**	means the range of marks that may be given to a Candidate or Bidder depending on the quality of its response to a question, which is located in the boxes below the applicable question
PROC023	**Organisation**	means a sole trader, partnership, limited partnership, limited liability partnership, co-operative or company and any analogous entity established inside or outside the UK and should be interpreted accordingly
PROC024	**PCR 2015**	means the Public Contracts Regulations 2015 (as amended)
PROC025	**PIN**	means the Prior Information Notice, relating to the entire Rainbow Programme, published by the Director on FTS on 11 March 2021, ref: 2021/S 000-004961
PROC026	**Procurement Documents**	means any document issued by the Director as part of this procurement process
PROC027	**Portal**	means the "Panacea" electronic procurement portal: [insert portal link] that will be used by the Director for receiving SQ and Bid submissions and managing all correspondence in relation to all stages of this procurement process
PROC028	**Proposed Contract**	means the Proposed Contract for Digital Integration and Service Operations as described in the Contract Notice and detailed in the Procurement Documents
PROC029	**Qualified Candidate**	means a Candidate which has been assessed as meeting the minimum requirements for participation
PROC030	**Selection Criteria**	means criteria used by the Director to determine whether a Candidate meets minimum requirements for participation in the procurement process in accordance with Regulation 58 of PCR 2015
PROC031	**Shortlisting Criteria**	means criteria used by the Director to determine which of the Candidates meeting the minimum requirements for participation shall be shortlisted to progress to the ISIT stage in accordance with Regulation 65 of PCR 2015

PROC032	**SQ**	means the Selection Questionnaire which Candidates must complete and return in order to participate in the selection stage
PROC033	**Statement of Requirements**	means the specification setting out the Director's needs and requirements for the Proposed Contract. Referred to as "the Services Description" as set out in Schedule 2.1 (Services Description)
PROC034	**Sub-Contractor**	Sub-contract means any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof. Sub-contractor means any third party with whom: (a) the Supplier enters into a Sub-contract; or (b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party; There is also the concept of a "Key Sub-Contractor" under the Agreement: Key Sub-contractor means any Sub-contractor: (a) which, in the opinion of the DirectorDirector, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Agreement (as set out in the Financial Model);
PROC035	**Supplier**	means the successful Supplier that has been awarded the Proposed Contract following the conclusion of the procurement process
PROC036	**Total Score Available**	means the maximum potential score that can be awarded for a response to a question

IT Definitions

#	Term	Description
IT001	***Amazon Web Services (AWS)***	*Amazon Web Services is a suite of cloud computing services that make a comprehensive cloud platform offered by Amazon.com.*
IT002	***Application Programming Interface (API)***	*An application programming interface (API) is an interface that allows the user to access information from another service and integrate this service into their own application.*

IT003	***Authentication***	*The process of gaining access to computer systems by reasserting an established trust relationship through the exchange of previously created Authentication Credentials*
IT004	***Bandwidth***	*A measurement of the amount of data that can be transmitted over a network at any given time.*
IT005	***BIAN***	*Banking Industry Architecture Network. Standards which enable banking interoperability.*
IT006	***Bring Your Own Device (BYOD)***	*An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.*
IT007	***Business Continuity***	*Activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.*
IT008	***BYOD***	*Bring Your Own Device or "BYOD" is a business and technology policy that allows employees to bring in personal mobile devices and use these devices to access company data, email, etc.*
IT009	***CMDB***	*Configuration Management Database*
IT010	***CMO***	*Current Mode of Operation. Used to describe systems and services provided by the incumbent today.*
IT011	***Customer Record***	*The record containing the Customer Level Data for a Customer*
IT012	***Data At Rest***	*Describes data in persistent storage such as hard disks, removable media or backups.*
IT013	***Data Migration***	*The process of moving data between two or more storage systems, data formats, warehouses or servers.*
IT014	***DDoS Attacks***	*A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic to a web property. In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.*
IT015	***Devices***	*Input devices include things like microphones, keyboards, mouse, touchpads, wheels, joysticks, etc. Output devices include printers, monitors, projectors and speakers.*
IT016	***DevOps***	*An amalgamation of "development" and "operations," DevOps is the combination of tasks performed by an organization's applications development and systems operations teams.*

IT017	***DHCP***	*Dynamic Host Configuration Protocol; a protocol that lets a server on a local network assign temporary IP addresses to a computer or other network devices.*
IT018	***Digital Banking Experience Platform***	*Technology capability which accelerates delivery of retail banking use cases to a range of digital touchpoints, including: apps; web; voice assistants.*
IT019	***Digital Customer Profile***	*The information NS&I requires to do business with customers through Digital Self-Service and Assisted Digital, market to customers digitally, and communicate with them digitally.(For example: Mandatory Customer Data; Regulatory consents and permissions; Registered device(s); and Authentication Credentials)*
IT020	***Disaster recovery***	*Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity.*
IT021	***DNS***	*The domain name system is how computers convert human-readable domain names and hostnames to numerical IP addresses.*
IT022	***EDIFACT***	*Electronic Data Interchange for Administration, Commerce and Transportation. An international standard for electronic data interchange.*
IT023	***Elasticity***	*In cloud computing, elasticity is a term used to reference the ability of a system to adapt to changing workload demand by provisioning and deprovisioning pooled resources so that provisioned resources match current demand as well as possible.*
IT024	***Electronic Random Number Indicator Equipment (ERNIE)***	*The system and software that generates random numbers used by the Prize Draw System to select Premium Bond prize winners*
IT025	***Encryption***	*The manipulation of data to prevent accurate interpretation by all but those for whom the data is intended.*
IT026	***End User Device (EUD)***	*Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.*
IT027	***Endpoint security***	*Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns.*
IT028	***Enterprise Application***	*An enterprise application is an application (or software) that is intended for large scale use by a (large) business.*

IT029	***Evergreen IT***	*An IT management approach that emphasises making small, iterative updates to an organisation's IT landscape (including desktop hardware, operating systems, products, applications, and infrastructure) on an ongoing basis rather than undertaking isolated big bang migrations. Enables running of services based on an IT estate which is always up-to-date and compliant.*
IT030	***Firewall***	*A firewall is a piece of software or hardware which uses a defined rule set to constrain certain types of traffic in order to prevent unauthorised access to/from a network. For example, a firewall could block incoming traffic on a certain port or block all incoming traffic except traffic coming from a specific IP address.*
IT031	***First in First Out***	*Queue that operates on a first-in, first-out (FIFO) principle. This means that the request is processed in the order in which it arrives.*
IT032	***Future Operating Model***	*Describes how Director will do business in the future. Enables the corporate vision to be translated into operations.*
IT033	***GDPR***	*The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).*
IT034	***Horizon Scanning***	*The early detection and assessment of emerging opportunities, issues threats or risks, such as new technologies available or emerging standards and legislations, which can be fed into continual improvements to the solution.*
IT035	***Hybrid Cloud***	*A hybrid cloud is a cloud computing environment that is comprised of a mix of private cloud, public cloud, and on-premises solutions.*
IT036	***IDAM***	*Identity and Access Management*
IT037	***Insight***	*Insight is generated using an understanding of the business context, expertise in analysis, learning and general reasoning skills to draw conclusions from the analysed data and information that can influence decisions and drive change.*

IT038	***Integration Layer***	*The Integration Layer sits at the centre of the to-be architecture, providing a bridge between all of the platforms. Its purpose is to take the commodity services which Director procure, and bring them together to "make" Director.* *The Intgeration Layer enables the decoupling of all platforms which make up the target estate, provides foundation connectivity, routing, and security capabilities.*
IT039	***Knowledge***	*Knowledge is generated by analysing data and information using methods and tooling.*
IT040	***Legacy***	*Used to describe services, processes, governance, systems, applications, technology and infrastructure provided by Atos, the incumbent supplier. Solution is still in use, but will be transformed as part of the Rainbow programme.*
IT041	***Load Balancing***	*The process of distributing computing workloads across multiple resources, such as servers. In cloud computing, a load balancer acts as a reverse proxy and distributes application traffic to multiple servers in order to prevent any single application server from becoming a point of failure.*
IT042	***Macro***	*A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.*
IT043	***Managed Service Provider (MSP)***	*A managed services provider (MSP) is an IT services provider that provides fully outsourced network, application, and system services across a network to clients.*
IT044	***Metadata***	*Data about data – that is, data describing the structure, content or use of some other data.*
IT045	***Middleware***	*Middleware is software that connects software components or enterprise applications.*
IT046	***Multi-Cloud***	*A multi-cloud strategy is the concurrent use of separate cloud service providers for different infrastructure, platform, or software needs.*
IT047	***Multi-Factor Authentication (MFA)***	*An Authentication method in which a user is granted access only after successfully presenting multiple factors from:* *Knowledge: something you know, eg a password* *Possession: something you have, eg a device* *Inherence: something you are, eg a biometric*
IT048	***Multi-Tenancy***	*Multi-Tenancy is a mode of operation for software in which multiple instances of one or many applications run in a shared environment.*

IT049	***Network Operations Center (NOC)***	*A network operations center, also known as a "network management center", is one or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication or satellite network.*
IT050	***OAT***	*Operational Acceptance Testing is an ITIL standard term*
IT051	***OAuth2.0***	*Standard used for authorisation of access to resources across applications.*
IT052	***Open Source***	*Computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source.*
IT053	***Operational Health Dashboard***	*Provides a visual of performance against KPIs. Helps an organisation understand, in real-time, if its performance is on target.*
IT054	***Orchestration Layer***	*Delivered by the incumbent supplier. Layer which creates the connections/instructions between third-party applications and the connector.* *To be replaced with the Integration Layer which will sit at the centre of the to-be architecture, providing a bridge between all of the platforms and enabling the decoupling of all platforms which make up the target estate.*
IT055	***Package A***	*Refers to the "Digital Integration and Service Operations" procurement package being tendered as part of the Director Rainbow programme.*
IT056	***Patching***	*Applying updates to firmware or software to improve security and/or enhance functionality.*
IT057	***Platform***	*The basic hardware (device) and software (operating system) on which applications can be run.*
IT058	***Prize Draw System***	*The system and software that uses random numbers from ERNIE to select Premium Bond prize winners*
IT059	***Ransomware***	*Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.*
IT060	***Router***	*A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.*
IT061	***RTO***	*Recovery Time Objective - the amount of real time a business has to restore its processes at an acceptable service level after an incident/disruption to avoid intolerable consequences associated with the disruption.*

IT062	***Scalability***	*Scalability is the ability of a process, system, or framework to handle a growing workload. In other words, a scalable system is adaptable to increasing demands.*
IT063	***Service Level Agreement (SLA)***	*A service level agreement (SLA) is a contractual agreement between a customer and a client which defines the level of service, availability and performance.*
IT064	***Service Stubs***	*Simulations of an actual service, which can be used to functionally replace the service in a test environment.*
IT065	***SIAM***	*Service Integration and Management. An approach to managing multiple suppliers of services (business services as well as information technology services) and integrating them.*
IT066	***SMAT***	*Service Management and Testing is an ITIL standard term*
IT067	***SMT***	*Service Management Toolset. Tools which help regulate how IT services are delivered within an organisation, based on budgets, people, processes, and outcomes.*
IT068	***SSO***	*Single Sign On*
IT069	***Transition State***	*A stable point in time where clear and measurements improvements are made to a service via the delivery of capability enhancements.*
IT070	***User Experience (UX)***	*The nature of a user's interaction with and perception of a system.*
IT071	***User Interface (UI)***	*User interface (UI) is the way that the user and computer system interact.*
IT072	***Vendor Lock-in***	*Vendor lock-in is when a customer finds themselves "locked-in" or stuck with a certain provider.*
IT073	***Virtual Machine (VM)***	*A virtual machine is a software computer that runs an operating system or application environment, just as physical hardware would.*

Business Definitions

#	Term	Description
Bus001	***Accessibility by Design***	*The design process in which the needs of people with disabilities are specifically considered*
Bus002	***Accessibility Criteria***	*A list of conditions that a user interface must meet to be considered accessible.* *The full name of the accessibility regulations is the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.*
Bus003	***Account***	*An holding held by a Customer or Trust in an NS&I Product*
Bus004	***Account Level Data***	*Information related to a Customer's Account(s), including: balances, transactions, investments, and prizes*

Bus005	***Accounts***	*A record or statement of financial expenditure and receipts relating to a particular period or purpose*
Bus006	***Agent***	*Any personnel who has voice or Digital contact with a Customer*
Bus007	***Agent Desktop***	*Defined as an intuitive tool that enables agents to communicate with customers*
Bus008	***AML***	*Anti money laundering - refers to the employment screening and customer due diligence to ensure that candidates and customers are not attempting to launder money through NS&I.*
Bus009	***Assisted Digital***	*The provision of support to Customers unable to self-serve digitally, to guide them through their Digital Self-Service journey or operate it on their behalf*
Bus010	***Authenticated Retail Website***	*The Customer-facing website, enabling Digital Self-Service for Authenticated Customers (aka Transactional Website)*
Bus011	***Authorised customer***	*Customers that have been authorised*
Bus012	***Back Office***	*Defined as the office or centre in which the processing of non digital customer services is carried out*
Bus013	***BACS***	*Defined as an electronic system to make payments directly from one bank account to another*
Bus014	***Bereavement Service***	*The Bereavement Service manages the process in the event of a customer's death for payment to the person entitled to the money*
Bus015	***CAB***	*Change Acceptance Board*
Bus016	***Case Base***	*A case base is similar to a knowledge article, except that details relating to specific issues, and their resolutions, are stored so that agents can refer to them in order to quickly resolve new occurrences of the same or similar issue". How does that sound*
Bus017	***Case Management***	*Defined as identifying, monitoring, managing and resolving customer cases*
Bus018	***CCA***	*Industry wide recognised accreditation programme, demonstrating a professional commitment to customer service*
Bus019	***Change of details service***	*The service enabling customers to change their account and personal details.*
Bus020	***Channel***	*The medium of interaction between the Customer and NS&I. Touchpoints are delivered by Channels.*
Bus021	***CHAPS***	*Defined as payments to UK accounts that are guaranteed to arrive on the day they are made*
Bus022	***Chat***	*Systems and services that enable Customers to communicate in real-time with Agents and/or Chatbots using text and/or voice-recognition/speech synthesis, via web/mobile/voice interfaces*
Bus023	***Chatbot***	*A software application used to automate Chat conversations in lieu of, or to supplement, direct contact with a live human Agent*

Bus024	***Co-Browsing***	*The joint navigation through online channels between the Agent and Customer*
Bus025	***Complaint management service***	*The system we currently use call charter which holds all the complaints data*
Bus026	***Contact***	*Defined as communication with (someone), typically in order to give or receive information.*
Bus027	***Contact Centre***	*The Contact Centre where Customers interact with Agents including chat, voice calls, messaging, e-mail and other forms of direct communication*
Bus028	***Content Strategy***	*A strategy for planning , creation, delivery, and governance of content.*
Bus029	***CSAT***	*Defined as a key performance indicator that tracks how satisfied customers (Customer Satisfaction)*
Bus030	***CSAT***	*Is a key performance indicator that tracks how satisfied customers are (Customer Satisfaction)*
Bus031	***Customer***	*An individual or organisation who is either: - an existing, prospective or past holder of a Product or recipient of a Service; or - a third party acting on behalf of a Customer (for example: a "Responsible Person", as defined in the Product Terms and Conditions; a Financial Advisor; a solicitor; or an executor).*
Bus032	***Customer Data***	*Data relating to a Customer, including their Customer Level Data and Account Level Data*
Bus033	***Customer Interaction***	*A Customer Interaction is a communication or transaction that occurs between a customer and NS&I via a customer touchpoint, communication channel or transactional interface.*
Bus034	***Customer Journey***	*A Customer Journey is made up of a series of Touchpoints.*
Bus035	***Customer Level Data***	*Information relating to an individual Customer (excluding their Account Data), including personal details, contact history, externally available information, and modelled values*
Bus036	***Customer Output***	*A communication sent to a Customer, by any Channel, including letters, forms, statements, leaflets, sales brochures, envelopes, certificates or records of investment, pre-recorded announcements, and Lines to Take*
Bus037	***Customer Persona***	Personas answer the question 'Who are we designing for?', and help to align our strategy and goals to specific user groups. NS&I have developed Personas for each of our Target Customer Segments and help bring our customers to life by describing their needs, goals, motivations and frustrations
Bus038	***Customer record***	*Holds critical data about a customer and its standard fields*
Bus039	***Customer Related Documents***	*All records of document composition; all items received from customers; and any item or communication sent to customers that cannot be fully reconstructed solely from records in the contact history*
Bus040	***Customer Value Proposition***	*Describes why a Customer would choose NS&I's Products or Services.*

Bus041	***Digital Champion***	*Defined as a digital SME who champions all things digital with agents to lift and improve an agents digital knowledge and confidence to help them support the business vision and their engagement with customers*
Bus042	***Digital Channels***	*Channels where Customers interact directly with NS&I using digital devices, including the Mobile Channel, the Internet Channel, voice assistants, chat and chatbots, social media, and Digital Communications*
Bus043	***Digital Communications Channels***	*Channels which enable digital communications between NS&I and Customers, including SMS, push notifications, messaging, email, and Secure Messages*
Bus044	***Digital Customer Profile***	*The information NS&I requires to do business with customers through Digital Self-Service and Assisted Digital, market to customers digitally, and communicate with them digitally. (For example: Mandatory Customer Data; Regulatory consents and permissions; Registered device(s); and Authentication Credentials)*
Bus045	***Digital Self-Service***	*To meet their needs, Customers self-serve end-to-end via Digital Touchpoints, with no unwanted deflection to post or phone, even for exceptions. Self-Service journeys are underpinned by straight-through automated processes with no human interaction or workarounds.*
Bus046	***Digital touchpoint***	*The combination of Digital Self-Service and Digital Channel.*
Bus047	***Digitally Excluded Customer***	*Someone who is unable to use NS&I's Digital Self-Service for any reason, including a lack of:* *• Access to digital technology* *• Capability to use digital technology* *• Engagement with digital technology* *• Skills and confidence in using digital technology*
Bus048	***Established saver***	*Target customer cohort. Customers in this cohort share some needs which underpin NS&I's Customer Value Proposition:* *• Mature financial experience* *• Generally older* *• Preference for longer term investments*
Bus049	***Evidence of Identity***	*Checks to verify a Customer's identity and postal address. The initial check is made electronically through a credit reference agency. If unsuccessful, the Customer provides Legal Documents or certified copies for back-office validation, chosen from a list of acceptable documents. These will be submitted digitally, with paper documents accepted by exception.*
Bus050	***Evidence of Identity service***	*The process to confirm that a customers' details are correctly identified (e.g. correctly identified home address, name etc).*
Bus051	***Excess refund process***	*The process to return funds to a customer that have taken the customers' account to holding over the acceptable product level*

Bus052	***Experience***	*How a Customer feels or we would like them to feel when using a Channel, Touchpoint, Service or considering purchasing a Product*
Bus053	***Fast Follower Status***	*Refreshes its capabilities in line with emerging hygiene factors and best practice for procured services*
Bus054	***Faster Payments***	*Electronic payments that can be made online or over the phone. Reduces payment times between different bank's customer accounts to typically a few seconds.*
Bus055	***FCA***	*The relevant regulatory bodies, including the Financial Conduct Authority and the Prudential Regulation Authority*
Bus056	***Financial Adviser***	*Defined as an individual who is regulated by the FCA to provide expert financial advice to consumers*
Bus057	***Financial Crime***	*Criminal activities carried out by individuals or criminal organisations to provide economic benefits through illegal methods*
Bus058	***Forgotten Security service***	*The process to re-enable a customer, once locked out of the service 9through forgetting password), to use the telephony and online service through resetting customer security details*
Bus059	***Future Project Activity Information***	*Refers to any plans the Supplier has to make changes to the operational service during the life of the contract, whether requested by the Director or carried out by the Supplier independently (e.g. applying regular patches).*
Bus060	***GDS***	*Government Digital Service*
Bus061	***General Correspondence service***	*The processing of a more complex or involved customer transaction (*including but not limited to, Power of Attorney, Court of Protection, Trusts, Independent Financial Adviser).
Bus062	***Help content***	*Help content is focused on helping people solve their problems and help them learn something new. It aims to get them interested in the brand not directly but by helping them learn more about the organisation and potentially become customers.*
Bus063	***High Value Prize***	*Currently any Premium Bond prize of £5,000 and over*
Bus064	***Identity Verification***	*The initial and ongoing checks, using Mandatory Data and Evidence of Identity provided by the Customer, to establish that a Customer, who has not previously been verified, is who they say they are and that they have passed regulatory due diligence, including Anti-Money Laundering and Know Your Customer checks*
Bus065	***Inclusive Design Principles***	*Designing for the needs of all people i.e. including those with permanent, temporary, situational, or changing disabilities. Inclusive design aims to remove the barriers that create undue effort and separation, enabling everyone to participate equally, confidently and independently in tasks or activities.*
Bus066	***Internet Channel***	*The retail internet Channel comprising of the Open Retail (marketing) Website and the Authenticated Retail (transactional) Website, and their supporting systems and services*

Bus067	***ITSCM***	*IT Service Continuity Management*
Bus068	***IVR/Voice Assistant***	*Defined as an automated phone system technology that allows incoming callers to access information via a voice response system of pre recorded responses without having to speak to an agent*
Bus069	***Jackpot (£1M)***	*Currently the largest monthly Premium Bond prize paid to an eligible winning customer*
Bus070	***Jobs To Be Done (JTBD)***	*A methodology for expressing the help that people want from services and products in their everyday lives. The facets of the model contextualise NS&I in our customers' lives and within the wider competitor landscape. Jobs to be Done applies to both our savings customers and our non-savings customers (e.g. proxies, bereavement claimants, children taking ownership of their account, etc). Combined with Moments that Matter, data and insight, this understanding allows us to prioritise which services to develop, find opportunities for improvement, and understand the impact of proposed changes to existing services.*
Bus071	***Key Control Indicator***	*Metrics designed to measure the adequacy of control around underlying Processes and business strategies. KCIs can identify process deviation from desired outcome.*
Bus072	***Key Risk Indicator***	*A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequences will exceed the organization's risk appetite and have a profoundly negative impact on an organization's ability to be successful.*
Bus073	***Knowledge Article***	*Defined as articles that are written and maintained by the Service Desk and are a way of providing staff and/or customers with a clear and common understanding of your services*
Bus074	***KYC***	*Know your customer - refers to the mandatory process of identifying and verifying a customer's identity when opening an account and periodically over time.*
Bus075	***Legal Documents***	*A document which the Director may require in respect of an Account, including: birth certificate; marriage certificate; death certificate; power of attorney; grant of probate; will; court of protection order; passport; change of name documentation; adoption certificate; any document sealed by the courts;*
Bus076	***Mass Customised/Customisation***	*To configure services and experiences so that they are tailored to the needs of target customer groups and/or personalised to the needs of individual customers.*
Bus077	***MI***	*Defined as Management information (MI) for analysis of trends, forecasting and solving problems*

Bus078	***MI***	*Management information (MI) for analysis of trends, forecasting and solving problems*
Bus079	***Missed opportunities***	*The prize that may occur as a result of things like late sales tat missed the cut off for the monthly prize draw or if there has been a business incident. The missed opportunity is the actual prize won on the reserve bond.*
Bus080	***Mobile Channel***	*The retail mobile device Channel, comprising of mobile apps and their supporting systems and services, enabling mobile access: to publicly available Product and general NS&I information; and Digital Self-Service for Authenticated Customers*
Bus081	***Moments That Matter***	*Moments in a customer's experience likely to have a significant impact on their level of satisfaction with the brand.*
Bus082	***MyLost Account***	*Defined as a service for customers to trace lost Accounts*
Bus083	***Omni Channel***	*A multichannel approach to sales that seeks to provide customers with a seamless customer experience*
Bus084	***Operational Processing***	*Defined as any non digital requests for completion of a service requested by a customer*
Bus085	***Orange Book***	*This guidance establishes the concept of risk management and provides a basic introduction to its concepts, development and implementation of risk management processes in government organisations*
Bus086	***Other Supplier(s)***	*Any supplier to the Director (other than the Supplier) which is notified to the Supplier from time to time and/or of which the Supplier should have been aware. Also includes any relevant third party supplier providing Related Services (i.e. PPA, PPC, PPD etc).*
Bus087	***Out of the Box***	*Ability to use the product, or a feature/functionality of a product without having to make any changes, special configuration or modification.*
Bus088	***Paperless Documents***	*The option where a Customer receives paperless Customer Outputs*
Bus089	***Payments***	*The term Payments may refer to any inbound, outbound, or internal movement of funds or ledger balances. Inbound Payment channels currently include bank transfer (Covering the BACS, Faster Payments, and CHAPS schemes), cheque and debit card. Outbound Payment channels include bank transfer (Covering the BACS, Faster Payments, and CHAPS schemes)*
Bus090	***Payments Service***	*Defined as the processing of a customer repayment application*
Bus091	***PCI DSS***	*Payment Card Industry Data Security Standard is defined as an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council*
Bus092	***Premium Bond Prize***	*A tax-free prize awarded at random in the monthly prize draw to a Customer holding Premium Bonds*

Bus093	***Prize Draw***	*A tax-free prize draw awarded at random in the monthly prize draw to a Customer holding premium bonds*
Bus094	***Proxy/Proxies***	*A Nominated person who can transact on the Account(s) of an NS&I Retail Customer on their behalf. An NS&I Retail Customer may grant responsibilities to a Proxy for a specific length of time or for a period with no specific end date.*
Bus095	***Public Retail Website***	*The Customer-facing website, containing publicly available Product and general NS&I information (aka Marketing Website)*
Bus096	***Quality Standards***	*Quality standards are defined as documents that provide requirements, specifications, guidelines, or characteristics that can be used consistently.*
Bus097	***Records Management service***	*An internal service which manages documentation including customer information and old signatures (held mainly on microfilm).*
Bus098	***Registration service***	*The process to register a customer to be able to use the online ad telephony service.*
Bus099	***Request for Information***	*A request for information or an apparent request under the FOIA or the Environmental Information Regulations*
Bus100	***Reserve Price List***	*Premium Bonds that are created as a result of late sales that missed the cut off for the monthly prize draw or if there has been a business incident. These can be used for a variety of reasons. Once the (reserve) bond is allocated it then has a retrospective prize check done on it to see if it should have won a prize in the earlier draw(s). If yes, then that prize is paid to the customer*
Bus101	***Return Undelivered service***	*The process to deal with any correspondence received that indicates a customer is no longer at the address we have on record.*
Bus102	***Sales Service***	*The processing of a customer purchase application.*
Bus103	***Scalable***	*The ability of a process, system, or framework to handle a growing workload. In other words, a scalable system is adaptable to increasing demands.*
Bus104	***Seamless Customer Experience***	*Where the customer journey is not impacted by any mistakes, delays, or setbacks in the event that a digital process is required to transition into a non-digital process or vice versa and is consistent across all channels*
Bus105	***Secure Message***	*Digital messaging between NS&I and Authenticated Customers via the Authenticated Website and/or Mobile Channel*
Bus106	***Service***	*An activity that helps a Customer to meet their needs*
Bus107	***Service Continuity Services***	*Encompasses business continuity, disaster recovery and insolvency continuity services.*
Bus108	***SIAM***	*Service Integration and Management*
Bus109	***SOP***	*Standard Operating Procedure*

Bus110	***Specialist complaints***	*Defined as complex cases, or cases whereby they may be in relation to Fraud, or with markers of vulnerability for the customer or accessibility requirements*
Bus111	***Starting saver***	*Those who are starting their savings journey have a strong propensity to save.*
Bus112	***Sub-Process***	*Defined as a process that supports delivery of the main customer services*
Bus113	***Supplier***	*Means the successful Supplier that has been awarded the Proposed Contract following the conclusion of the procurement process.*
Bus114	***Target customers cohorts (i.e. Established savers and Starting savers)***	*Target customers are those who have the positive behaviours and traits that align with NS&I's aspirations in Rainbow.*
Bus115	***Tone of Voice***	*Defined as the style in 'how' NS&I communicates with customers through written word and voice - underpinned by NS&I's brand values and CX principles.*
Bus116	***Touchpoint***	*An interaction between the Customer and NS&I through an exchange of information, provision of a Service or undertaking of a transaction via a channel and using a device. e.g. withdrawing money on the NS&I app on a mobile device.*
Bus117	***Tracing***	*The Director's own Service enabling Customers to trace lost Accounts*
Bus118	***True and Fair***	*True and Fair is the term using in the audit report of financial statements to express the condition that financial statements are truly prepared and fairly presented in accordance with the prescribed accounting standards*
Bus119	***User***	*Any person who is an authorised end user of the Services, the Supplier's System or other information system or application required to be provided as set out in the Director's Requirements.*
Bus120	***User centred design***	*An iterative design process in which designers focus on the users and their needs in each phase of the design process. Includes the involvement of users throughout the design process via a variety of research and design techniques, to create highly usable and accessible products for them.*
Bus121	***Vulnerable Customer***	*This definition follows the FCA definition: someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.* *4 key drivers may increase the risk of Vulnerability:* *Health – disabilities or illnesses that affect the ability to carry out day-to-day tasks* *Life events – major life events such as bereavement, job loss or relationship breakdown* *Resilience – low ability to withstand financial or emotional shocks* *Capability – low knowledge of financial matters or low*

		confidence in managing money (financial capability) and low capability in other relevant areas such as literacy, or Digital skills
Bus122	***WCAG***	*Web Content Accessibility Guidelines - The Web Content Accessibility Guidelines are part of a series of web accessibility guidelines published by the Web Accessibility Initiative of the World Wide Web Consortium*

Annex 2 PPC Requirement Catalogue

This package comprises of twelve headline commissioning requirements which have been broken down into stakeholder and service/solution requirements. These can be found on the tabs below.

Grouping	Requirement ID	Number of linked L2s	Number of linked L3s	Commissioning requirement
Contact Centre				
Assisted Digital	PPCL1-001	17	185	As NS&I Business Owner, I want the chosen supplier to provide an Assisted Digital service for our customers in alignment with our defined NS&I Digital Self-service Journeys, so that NS&I Customers, unable to digitally self-serve, are able to fully access our products and services
Back Office				
Non-Digital Operational Processing	PPCL1-002	22	78	As NS&I Business Owner, I want the new supplier to provide any non-digital operational processing required to support the delivery of customer services, so that NS&I is able to deliver the full suite of services that our customers expect
Complaints Management	PPCL1-003	14	77	As NS&I Business Owner, I want the new supplier to provide a complaints management service in accordance with regulatory standards, so that we can ensure customers get the service they expect, and any failures in services are remediated
Document Management	PPCL1-004	14	93	As NS&I Business Owner, I want the new supplier to provide a document production, storage and management service, so that NS&I can meet its accessibility obligations relating to digitally excluded / vulnerable customers
Non-Digital Prize Draw	PPCL1-005	4	25	As NS&I Business Owner, I want the new supplier to provide any non-digital Prize Draw related operational processing, so that all prizes are allocated. exceptions resolved and customers notified
Architecture & Integration				
Risk and Compliance	PPCL1-006	6	24	As NS&I Business Owner, I want the new supplier to operate its defined and agreed customer services in accordance with all relevant risk frameworks and compliance legislation, so that NS&I delivers a trustworthy and safe customer experience
SIAM	PPCL1-007	38	167	As the NS&I Business Owner, I want the new supplier to work with the NS&I SIAM function and other suppliers to deliver our services, so that customers journeys are seamless across the multi-supplier model
Security	PPCL1-008	9	306	As NS&I Business Owner, I want the new supplier to operate in a manner which protects NS&I customers from security threats and attacks, so that NS&I's brand and reputation are maintained
Architecture	PPCL1-009	19	172	As the NS&I Business Owner, I want the new supplier to develop and operate its services in accordance with NS&I architectural design standards, including utilisation of any prescribed technologies, so that NS&I remains architecturally coherent and services can easily be re-procured in the future
Competitor, Service and Customer Intelligence	PPCL1-010	6	68	As a Business Owner, I want the new supplier to provide NS&I with relevant competitor, service and customer intelligence, so that NS&I can continuously improve its propositions and services
Transformation	PPCL1-011	1	12	As NS&I Business Owner, I want the new supplier to promote adoption of digital services so that NS&I can move from current to future operating model.
Financial Crime	PPCL1-012	10	60	As a Business Owner, I want the new supplier to provide financial crime investigation and management services, so that NS&I can meet obligations to protect it's customers and minimise losses through fraudulent activity.
Total requirements		**160**	**1233**	

L2 Requirement ID	Number of linked L3s	Link to L1	Date	Grouping	Current Requirement (incl. the 'what' and the 'why')	Previous requirement
PPCL2-SEC-001		PPCL1-008	#########	Security	The Supplier shall follow good security practice during implementation and throughout the life of the contract to enable business operations to be conducted in a secure manner and in line with the Directors requirements and standards.	
PPCL2-SEC-002		PPCL1-008	#########	Security	The Supplier shall ensure that all of the Director's services across all channels are secured in line with the Directors requirements and standards.	
PPCL2-SEC-003		PPCL1-008	#########	Security	The Supplier shall ensure the customer and user access to the systems and applications is authenticated and authorised so that the Director can maintain confidentiality, integrity and availability	
PPCL2-SEC-004		PPCL1-008	#########	Security	The Supplier shall ensure that information is exchanged securely with other services and organisations, so that the confidentiality, integrity and availability of the solution and its information is protected at all times.	
PPCL2-SEC-005		PPCL1-008	#########	Security	The Supplier shall implement measures to protect the Director's brand and activities so that customers are reassured that they are safe, and their information is secure when accessing the Director's contact centre support services.	
PPCL2-SEC-006		PPCL1-008	#########	Security	The Supplier shall provide logs and event data to the Director's security monitoring solution so that attacks can be detected and responded to in a timely manner.	
PPCL2-SEC-007		PPCL1-008	#########	Security	The Supplier shall ensure design and development activities are undertaken securely so that deployments or any significant changes are done securely and do not pose a security threat to the Director's wider ecosystem.	
PPCL2-SEC-008		PPCL1-008	#########	Security	The Supplier shall be willing to provide the information needed to the Director to prove security of activities being undertaken, so that the Director has adequate assurance that sufficient and adequate security measures are being implemented.	
PPCL2-SEC-009		PPCL1-008	#########	Security	The Supplier shall design and implement a business continuity management system (BCMS) certified independently to ISO 22301 standards which covers the scope of all services provided and is accepted by the director.	
PPCL2-SIM-001		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the Availability Management Policies and Procedures so that SIAM can ensure that the availability levels for all services comply with or exceed the agreed requirements in a cost-effective manner	
PPCL2-SIM-002		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the Capacity Management Policies and Procedures so that SIAM can ensure that appropriate levels of resources and system performance are set and delivered, meeting the needs of the Director	
PPCL2-SIM-003		PPCL1-007	#########	SIAM	The Supplier shall monitor all events that occur, notifying the Director's SIAM function when it becomes aware of a potential Service Impacting Event so that exceptional conditions can be detected and escalated appropriately	
PPCL2-SIM-004		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the IT Service Continuity Management Policies and Procedures so that emerging ITSCM risks or threats are mitigated to support business continuity	
PPCL2-SIM-005		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the Service Asset and Configuration Management Policies and Procedures so that accurate asset and configuration data is maintained	
PPCL2-SIM-006		PPCL1-007	#########	SIAM	The Supplier shall provide all relevant information, including the detail, status, possible interactions and mutual dependencies, of all current services and those under development so that the Director's SIAM function is informed in the development, maintenance and distribution of the service catalogue	
PPCL2-SIM-007		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the Service Level Management Policies and Procedures so that accurate service level management information and appropriate supporting documentation is provided	
PPCL2-SIM-008		PPCL1-007	#########	SIAM	The Supplier shall adhere to the Director's SIAM function policies and procedures that define standards and architecture so that operational standards and criteria are consistent and adhered to, providing an effective reference point for implementing and transitioning services	
PPCL2-SIM-009		PPCL1-007	#########	SIAM	The Supplier shall provide the Director's SIAM function with a feed of information according to the Financial Management Policies and Procedures so that the consumption of chargeable resources, catalogue requests and other change requests service charges can be validated	
PPCL2-SIM-010		PPCL1-007	#########	SIAM	The Supplier shall deliver services which are compliant with agreed service management policies, procedures and processes so that there is a consistent quality of service provision	
PPCL2-SIM-011		PPCL1-007	#########	SIAM	The Supplier shall identify named individuals to act as client relationship managers so that interfaces into the SIAM function and the Directors core functions are as seamless as possible	
PPCL2-SIM-012		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function Service Desk by ensuring all relevant information is provided when contacts are made so that the service desk can deliver efficiently and maintain good management of the case	
PPCL2-SIM-013		PPCL1-007	#########	SIAM	The Supplier shall provide an effective data integration with the Director's SIAM function service desk tool(s) to facilitate incident management so that service availability, incident severity and resolution time metrics are met	
PPCL2-SIM-014		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function with defining and executing the Service Request Management Policies and Procedures so that service requests are accurately captured, assigned and fulfilled	
PPCL2-SIM-015		PPCL1-007	#########	SIAM	The Supplier shall cooperate with the Director's SIAM function and other service providers on problem investigations so that problems are correctly identified and escalated	
PPCL2-SIM-016		PPCL1-007	#########	SIAM	The Supplier shall adhere to access management policies and procedures set by the Director's SIAM and/or security functions so that access to data and functionality is controlled appropriately.	
PPCL2-SIM-017		PPCL1-007	#########	SIAM	The Supplier shall ensure that all relevant service management information is made available to the Director's SIAM function so that the development of the service knowledge management repository is comprehensive	
PPCL2-SIM-018		PPCL1-007	#########	SIAM	The Supplier shall support the Director and its SIAM function with the service level design review so that the definition of the service levels, service targets and KPIs are clear and periodic audit reviews can take place	
PPCL2-SIM-019		PPCL1-007	#########	SIAM	The Supplier shall comply with the Service Management Policies and Procedures, including regulatory obligations, required by the Director's SIAM function and ensure that any non-compliance is raised and managed through to resolution	
PPCL2-SIM-020		PPCL1-007	#########	SIAM	The Supplier shall collaborate with the Director's SIAM function and other Suppliers to support Service Transition activities, so that they are aware of and approve their specific responsibilities of activity needed to deliver the transition or change successfully Service Transition activities include but are not limited to: service transition planning, integration testing and service evaluation	
PPCL2-SIM-021		PPCL1-007	#########	SIAM	The Supplier shall assist the Director's SIAM function in the definition and execution of Change Management Policies and Procedures so that change is monitored and managed efficiently between Suppliers and the Director, reducing negative impacts	
PPCL2-SIM-022		PPCL1-007	#########	SIAM	The Supplier shall participate in scheduling releases with the Director's SIAM function and other service providers so that all Suppliers are informed of the plan allowing deployments to run smoothly	
PPCL2-SIM-023		PPCL1-007	#########	SIAM	The Supplier shall provide enhanced support post-deployment so that operations after new or changed services are smoothly delivered, ensuring swift remediation of issues	
PPCL2-SIM-024		PPCL1-007	#########	SIAM	The Supplier shall support the Director's SIAM function and other service providers with integration testing with so that testing is effective and ensures that all the service providers' components are integrated to provide the Director with stable, maintainable end-to-end service	
PPCL2-SIM-025		PPCL1-007	#########	SIAM	The Supplier shall provide future project activity information so that the Director's SIAM function can assess and schedule future test environment availability	
PPCL2-SIM-026		PPCL1-007	#########	SIAM	The supplier shall lease with the Director's SIAM function to align project portfolio and services to enterprise strategy, risk and security requirements and ensure outcomes delivered by multiple suppliers so that services are coherent and end-to-end	
PPCL2-SIM-027		PPCL1-007	#########	SIAM	The Supplier shall integrate and contribute to the Directors mandated knowledge management and collaboration tooling so that a central repository of corporate information is maintained	
PPCL2-SIM-028		PPCL1-007	#########	SIAM	The Supplier shall ensure that they have a comprehensive business continuity, Disaster recovery and Backup strategy and plan so that the Director's services are able to tolerate and recover from major events	
PPCL2-SIM-029		PPCL1-007	#########	SIAM	The Supplier shall contribute to an end-to-end Service Transition Approach and detailed plan to evidence their approach and activities required to transition services to its target state. Transition approach must be low risk, smooth, successful and have minimal impact on customers and the Director.	
PPCL2-SIM-030		PPCL1-007	#########	SIAM	The Supplier shall align with the cross-supplier collaborative ways of working so that the Director and its suppliers can work efficiently to achieve their common aims	
PPCL2-SIM-031		PPCL1-007	#########	SIAM	The Supplier shall support the Director in delivering insight-driven continuous improvement and delivery so that the Director can improve services frequently, iteratively and cost-effectively	
PPCL2-SIM-032		PPCL1-007	#########	SIAM	The Supplier shall ensure delivery and continuous improvements are driven by actionable insight into business drivers, end-to-end service needs, and operational performance so that the Director reduces the risk and maximises the effectiveness of service	
PPCL2-SIM-033		PPCL1-007	#########	SIAM	The Supplier shall operate with appropriate levels of devolved authority so that teams are self-sufficient and empowered to act on insight and can prioritise their deliverables	
PPCL2-SIM-034		PPCL1-007	#########	SIAM	The Supplier shall communicate with the Director and its Suppliers, sharing knowledge openly and transparently so that teams are empowered and have the information they need to make decisions	
PPCL2-SIM-035		PPCL1-007	#########	SIAM	The Supplier shall align with the Director's service governance so that the accountabilities and responsibilities for change and its risks, are clearly defined, understood, and managed	
PPCL2-SIM-036		PPCL1-007	#########	SIAM	The Supplier shall align with the Director's cadence of delivery so that management and delivery of service is coordinated across Suppliers, vendors, release paths, and touchpoints	
PPCL2-SIM-037		PPCL1-007	#########	SIAM	The Supplier shall leverage competitor and market intelligence so that the Director can maintain its fast follower status so that it refreshes its capabilities in line with emerging hygiene factors and best practice for procured services	
PPCL2-SIM-038		PPCL1-007	#########	SIAM	The Supplier shall provide end-to-end reporting and monitoring capabilities, so that the Director has oversight over operations and security of the solution	
PPCL2-ART-001		PPCL1-009	#########	Architecture	The Supplier shall design, build and operate the procured solutions in collaboration with other Supplier solutions by participating in the Director's Design Governance Processes. This shall be done across the Transition States and beyond, so that seamless end-to-end services are delivered.	
PPCL2-ART-002		PPCL1-009	#########	Architecture	The Supplier shall make available to the Director resources and documentation relevant to its intellectual property, so that the Director has access to information required to run and maintain the solution being procured. Information and documentation includes but is not limited to: configurations used, code repository, design documentation, escrow arrangements	
PPCL2-ART-003		PPCL1-009	#########	Architecture	The supplier shall design solutions in accordance with the Directors architectural standards and principles so that the Director enterprise architecture has design coherence.	
PPCL2-ART-004		PPCL1-009	#########	Architecture	The supplier shall utilise Directors prescribed technologies, where appropriate, so that the Director can have an integrated estate of services.	
PPCL2-ART-005		PPCL1-009	#########	Architecture	The supplier shall design, build and operate the procured solutions in collaboration with other Supplier solutions so that seamless end-to-end services are delivered.	
PPCL2-ART-006		PPCL1-009	#########	Architecture	The supplier shall provide resilient solutions so that services to the Director's customers are available as much as possible.	
PPCL2-ART-007		PPCL1-009	#########	Architecture	The supplier shall comply with the non-functional characteristics of the Directors requirements so that the services meet the business needs.	
PPCL2-ART-008		PPCL1-009	#########	Architecture	The Supplier shall provide all infrastructure and development environments required (hardware and software), so that the platform is not reliant on the Director's provided infrastructure.	
PPCL2-ART-009		PPCL1-009	#########	Architecture	The Supplier shall provide change management capabilities so that the customer and business outcomes from the solution are continuously improved.	
PPCL2-ART-010		PPCL1-009	#########	Architecture	The Supplier shall ensure that each element of their solution is designed & tested for accessibility, so that staff are able to complete their "Jobs to be done".	
PPCL2-ART-012		PPCL1-009	#########	Architecture	The Supplier shall work collaboratively with other Suppliers to carry out and support migration activities, so that any required data migrations can be carried out in a reliable and efficient manner.	
PPCL2-ART-013		PPCL1-009	#########	Architecture	The solution shall provide monitoring capabilities, so that the Director has oversight over operations and security of the solution.	
PPCL2-ART-014		PPCL1-009	#########	Architecture	The Supplier shall provide insights into how they are developing their product roadmap, so that the Director can be assured that the product suite is being actively developed and that the roadmap aligns with the Director's strategic vision.	
PPCL2-ART-015		PPCL1-009	#########	Architecture	The Supplier shall continuously share with the Director any expected changes to roadmaps, so that the Director can perform the required market/competitor analysis before any products are developed and are aware of any upcoming changes which can be in turn prioritised.	
PPCL2-ART-016		PPCL1-009	#########	Architecture	The Supplier's solution shall enable intelligence from individual capabilities to be combined with data and intelligence from other areas of the business, so that it can be analysed for reporting and to develop new insights which inform recommendations for improving the customer experience.	
PPCL2-ART-018		PPCL1-009	#########	Architecture	The Supplier's solution shall provide actionable insight into operation and service issues, so that the Director is able to understand what the problems are and what to do about them.	
PPCL2-ART-019		PPCL1-009	#########	Architecture	The Supplier shall maintain versions of Solution's components and services at mainstream supported levels, so that the Director has minimised security and design flaw exposure	
PPCL2-ART-020		PPCL1-009	#########	Architecture	The Supplier shall ensure the accuracy and integrity of all data within their provisioned services, so that the customer and operational journey remains positive and the Director fulfils its HM Treasury requirements	
PPCL2-ART-021		PPCL1-009	#########	Architecture	The Supplier shall collaborate with other Suppliers and the Director to ensure the end-to-end data consistency and integrity, so that the Director can deliver seamless end-to-end services	
PPCL2-AD-001		PPCL1-001	#########	Assisted Digital	The supplier shall provide a UK based, CCA accredited contact centre so that the assisted digital services can be delivered for the Director's customers who are unable to self-serve digitally.	
PPCL2-AD-002		PPCL1-001	#########	Assisted Digital	The supplier shall facilitate customers completing their Jobs To Be Done so that a customer can complete the journey with assistance from an agent completing interactions or elements of interactions.	
PPCL2-AD-003		PPCL1-001	#########	Assisted Digital	The supplier shall facilitate customers completing their Jobs To Be Done so that a customer can complete the journey with an agent completing interactions on their behalf.	
PPCL2-AD-004		PPCL1-001	#########	Assisted Digital	The supplier should provide a capability to identify whether a customer is vulnerable across channels so that the vulnerable customers can be assisted appropriately.	
PPCL2-AD-005		PPCL1-001	#########	Assisted Digital	The supplier shall provide core Assisted Digital services via multiple channels (such as Co-Browsing, Chatbot, Telephony, Social Media, etc) so that they are able to service the customers efficiently and create seamless positive customer experience including when customers move across the channels.	
PPCL2-AD-006		PPCL1-001	#########	Assisted Digital	The supplier shall provide any future proof Assisted Digital services and technologies (such as AI, ML, NLP, etc) via multiple channels so that they are able to service the customers efficiently and create positive customer experience.	
PPCL2-AD-007		PPCL1-001	#########	Assisted Digital	The supplier shall provide a telephony channel including IVR to support the delivery of assisted digital services so that the customers are able to engage with the Director via their channel of choice and complete their digital journeys.	

PPCL2-AD-008		PPCL1-001	#########	Assisted Digital	The supplier shall provide secure online communication secure chat to support the delivery of assisted digital services so that the customers are able to engage with the Director via their channel of choice to complete their digital journeys.	
PPCL2-AD-009		PPCL1-001	#########	Assisted Digital	The supplier shall provide an in-app call capability to the Director's mobile app so that customers can communicate securely with the Agents.	
PPCL2-AD-011		PPCL1-001	#########	Assisted Digital	The supplier shall provide support for customer payments in collaboration with other suppliers and in compliance with payment rules, regulations and policies so that the customers can make payment securely.	
PPCL2-AD-012		PPCL1-001	#########	Assisted Digital	The supplier shall ensure that all the customer conversations across digital and non-digital channels are responded to, in line with the Director's quality standards and content strategy so that customer's queries are resolved successfully and they have positive engaging experience.	
PPCL2-AD-013		PPCL1-001	#########	Assisted Digital	The supplier must ensure that the contact centre agents have skills, tools and access to data so that they can achieve closure with the customer interactions on a "one and done" basis.	
PPCL2-AD-014		PPCL1-001	#########	Assisted Digital	The supplier should provide the fully integrated Case management capability so that the agents can identify, monitor, manage and resolve customer cases.	
PPCL2-AD-015		PPCL1-001	#########	Assisted Digital	The Supplier provide an automated solution for the agents so that they are able to obtain answers to FAQs.	
PPCL2-AD-016		PPCL1-001	#########	Assisted Digital	The supplier shall support the customers use of assistive technologies to support customers with disabilities, restrictive mobility or other impairments so that these customers are serviced successfully and experience positive engaging interactions.	
PPCL2-AD-017		PPCL1-001	#########	Assisted Digital	The supplier shall provide the tools and run processes to obtain and monitor customer feedback so that these inputs can be included when improving services and providing insights to the director.	
PPCL2-AD-018		PPCL1-001	#########	Assisted Digital	The supplier shall work collaboratively with other suppliers to deliver end to end customer journeys across all channels so that service expectations are met.	
PPCL2-OPS-001		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall accurately execute operational processing of customer journeys, for example but not limited to the processes specified below (in requirements 2 - 13) which cannot be completed with the digital processes within appropriate timelines so that customers are provided with positive	
PPCL2-OPS-002		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Bereavement service, until such a point that, in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-003		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Sales service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-004		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Payments service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-005		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Proxies (including but not limited to, Power of Attorney, Court of Protection, Trusts, Independent Financial Adviser) service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer	
PPCL2-OPS-006		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Tracing (including those from My Lost account) service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-007		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the General Correspondence service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-008		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Change of details service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-009		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Records Management service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-010		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Return Undelivered service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-011		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Evidence of Identity service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-012		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Registration service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-013		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall provide operational processing for the Forgotten Security service, until such a point and in collaboration with other suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL2-OPS-014		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall execute operational processing of all customer journeys on behalf of customers unable to self-serve digitally so that such customers can complete their jobs to be done.	
PPCL2-OPS-015		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall ensure consistency in customer engagement experience between digital and non-digital journeys so that the Director can ensure equivalent experience for all customers.	
PPCL2-OPS-016		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall ensure reliable integration with other supplier(s') systems so that the supplier can securely communicate with customers digitally in relation to their interactions.	
PPCL2-OPS-017		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall integrate secure messaging with Customer Case Management to identify when a customer has responded so that the supplier knows action needs to be taken.	
PPCL2-OPS-018		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall design and provide appropriate means to meet customers' correspondence requirements in accordance with the Directors agreed approach so that the Director can effectively communicate to its customers.	
PPCL2-OPS-019		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall, in collaboration with other suppliers promptly provide data on request so that the Director can complete obligations such as HMT requests, parliamentary requests, data underpinning PI results, FOI etc. in a timely manner as agreed by the Director.	
PPCL2-OPS-020		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall, in collaboration with other suppliers, ensure customer journeys which cannot be completed in the digitised services are easily transitioned to operational processing for completion so that customer journeys can be completed efficiently with minimal disruption.	
PPCL2-OPS-021		PPCL1-002	#########	Non-Digital Operational Processing	The supplier shall automate non-digitised processes where appropriate so that operational processing can be completed in an optimal manner.	
PPCL2-CMP-001		PPCL1-003	#########	Complaints Management	The supplier shall record and resolve complaints in a timely manner In-line with agreed complaints framework adhering to FCA requirements, so that customer experience is improved.	
PPCL2-CMP-002		PPCL1-003	#########	Complaints Management	The supplier shall provide the capability to identify and register complaints received at first points of contact with all digital and non-digital channels including but not limited postal, telephone, social media etc. so that complaints are recognised and dealt with in a timely manner.	
PPCL2-CMP-003		PPCL1-003	#########	Complaints Management	The supplier shall design and deliver a defined complaints escalation process which is clear to the complaints operations team to follow so that they can effectively escalate complaints to the appropriate channels.	
PPCL2-CMP-004		PPCL1-003	#########	Complaints Management	The supplier shall deliver a complaint management service that supports effective ownership of reported issues so that actions are taken to rectify them within timelines agreed with the Director.	
PPCL2-CMP-005		PPCL1-003	#########	Complaints Management	The supplier shall deliver a process to support the Director to review and respond to specialist complaints including but not limited to HMT complaints, media complaints and MP complaints so that these high profile complaints can be managed appropriately.	
PPCL2-CMP-006		PPCL1-003	#########	Complaints Management	The supplier shall deliver a complaint management service that supports cross system alignment of customer details so that customer information is kept up to date across the service and with other suppliers' systems.	
PPCL2-CMP-007		PPCL1-003	#########	Complaints Management	The supplier shall ensure customer data is accessible in one place so that complaints operations team can easily view customer information and business correspondence.	
PPCL2-CMP-008		PPCL1-003	#########	Complaints Management	The supplier shall design and employ appropriate methods to manage policy/large incident related complaints, so that they can be dealt with efficiently and consistently.	
PPCL2-CMP-009		PPCL1-003	#########	Complaints Management	The supplier shall ensure compensation is awarded to customers in line with compensation policy so that the complaint is resolved appropriately.	
PPCL2-CMP-010		PPCL1-003	#########	Complaints Management	The supplier shall capture and monitor root causes of complaints in order to generate actionable insights and recommendations so that appropriate remediation can applied to improve customer experience.	
PPCL2-CMP-011		PPCL1-003	#########	Complaints Management	The supplier will produce FCA reporting in line with FCA requirements for the Director to approve prior to issuance and publication so that the Director can review, input and remain compliant with complaints reporting.	
PPCL2-CMP-012		PPCL1-003	#########	Complaints Management	The supplier shall collaborate with the Director to manage all FOS related queries so that oversight can be given to ensure all tasks are actioned.	
PPCL2-CMP-013		PPCL1-003	#########	Complaints Management	The supplier shall utilise complaints analysis to provide feedback and recommendations to specific business areas and staff in order so that reoccurrence is reduced and the service or process is continually improved.	
PPCL2-CMP-014		PPCL1-003	#########	Complaints Management	The supplier shall design and provide an effective data protection complaints management procedure, including specialists knowledge and training for staff and agreed timelines for resolution, so that the Director remains in compliance with the relevant legislation.	
PPCL2-DPM-001		PPCL1-004	#########	Document Management	The supplier shall provide a secure document storage and retrieval solution, so that documents received or issued can be stored and retained in line with the relevant regulatory (FCA), legal (data retention) and internal policies.	
PPCL2-DPM-002		PPCL1-004	#########	Document Management	The supplier shall digitise (e.g. scanning and OCR) inbound physical documentation received from customers so that requests for service can be efficiently provided via digital or automated means	
PPCL2-DPM-003		PPCL1-004	#########	Document Management	The supplier shall provide the capability to ingest, search, serve, modify and deploy different file types so that the Director can utilise files in alignment with defined processes and procedures.	
PPCL2-DPM-004		PPCL1-004	#########	Document Management	The supplier shall process inbound/outbound post to the agreed level of requirements (e.g. postal classification, security, secure storage, retention etc.), so that customer experience, operational processing and record keeping can be delivered to agreed standard.	
PPCL2-DPM-005		PPCL1-004	#########	Document Management	The supplier shall manage (e.g. identify, scan, categorise etc.) inbound paper documents and route them to the appropriate workflow for processing, so that customer experience, operational processing and record keeping can be delivered to agreed standard.	
PPCL2-DPM-006		PPCL1-004	#########	Document Management	The supplier shall produce customer correspondence in paper or electronic format (including secure messages) by using pre-agreed letters and/or component paragraphs, including but not limited to; templates, forms, brochures, so that the supplier can communicate with customers within parameters agreed with the Director.	
PPCL2-DPM-007		PPCL1-004	#########	Document Management	The supplier shall ensure that the document management solution integrates with other services, so that information and data is available to support the construction of correspondence and delivery of relevant processes across the enterprise.	
PPCL2-DPM-008		PPCL1-004	#########	Document Management	The supplier shall provide scalable printing capabilities for the various types and volumes of required outputs, so that the Director can correspond with customers in a timely manner.	
PPCL2-DPM-009		PPCL1-004	#########	Document Management	The supplier shall provide the capability to print, control and dispatch warrants with the appropriate security measures, so that customers who are unable to receive electronic payment can receive accurate payment from the director in timely manner.	
PPCL2-DPM-010		PPCL1-004	#########	Document Management	The supplier shall provide a template storage and management solution, so that documentation formats can be standardised, reviewed, amended and approved.	
PPCL2-DPM-011		PPCL1-004	#########	Document Management	The supplier shall deliver efficient, flexible, comprehensive testing and evidence of all electronic and printed documents newly specified by the Director and provide these to the Director for approval so that final print output can be assured as correct.	
PPCL2-DPM-012		PPCL1-004	#########	Document Management	The supplier shall manage the end-to-end processing of cheques including banking, scanning, reconciliation, returning and post processing (destroy, return to customer or retain in line with agreed retention policy) so that, customer payments and the Director's banking activities is appropriately	
PPCL2-DPM-013		PPCL1-004	#########	Document Management	The supplier shall ensure that structured, semi-structured data and metadata is available to be used within the Insights capability, so that the Director is able to make effective operational and customer decisions.	
PPCL2-DPM-014		PPCL1-004	#########	Document Management	The supplier shall enable for stored data/correspondence to be linked to a customer record so that the Director and its suppliers have a full view of the customer and history of customer's interactions with the Director.	
PPCL2-PD-002		PPCL1-005	#########	Non-Digital Prize Draw	The supplier shall operate and support the elements of the Jackpot (£1m) winner services including preparation of specialist documentation and payment arrangements so that the winner has the positive customer experience.	
PPCL2-PD-003		PPCL1-005	#########	Non-Digital Prize Draw	The supplier shall accurately execute operational processing of customer journeys related to Prize Draw, for example but not limited to the processes specified below (i.e. Missed Opportunities, Reserve Prizes, Excess Refund Processing), which cannot be completed with the digital processes, within	
PPCL2-PD-007		PPCL1-005	#########	Non-Digital Prize Draw	The supplier shall be able to make any permitted updates to the customer records as part of their interactions with the customers in the prize draw process / operations so that the accurate customer data is available and drives appropriate processes/adjustment in the Prize Draw process.	
PPCL2-PD-008		PPCL1-005	#########	Non-Digital Prize Draw	The supplier shall collaborate with the Director and other suppliers to ensure that all suppliers meet their specific responsibilities in conducting the prize draw successfully.	
PPCL2-RC-001		PPCL1-006	#########	Risk	The supplier shall operate a risk framework which meets the Government standard set out in the Orange Book and aligns as far as practicable with the Director's risk framework, so that the Director has assurance of risks being appropriately managed.	
PPCL2-RC-002		PPCL1-006	#########	Risk	The supplier shall provide real time access for the Director to comprehensive risk data, so that the Director has an accurate view of risk exposures.	
PPCL2-RC-003		PPCL1-006	#########	Risk	The supplier shall support any audit or assurance activities instigated by the Director both in the supplier operation and any approved subcontracting of services, so that the Director can be assured that work is being conducted to a high standard and in accordance with agreed contracts.	
PPCL2-RC-004		PPCL1-006	#########	Compliance	The supplier shall operate in compliance with the legislation relevant to the Director's business/operation, including, but not limited to, new, amended or extended legislation and any FCA requirements as would be required by a fully regulated deposit-taker, including the treatment of vulnerable customers and the handling of customer complaints, so that the Director can be assured that his legal and regulatory equivalence obligations are met,	The supplier shall operate in compliance with the legislation relevant to the Director's business/operation (as set out in the Compliance Universe document) so that the Director can be assured that his legal and regulatory obligations are met, and the risks associated with those obligations are managed appropriately
PPCL2-RC-005		PPCL1-006	#########	Compliance	The supplier shall ensure that their staff, and the staff of their sub-contractors, where applicable, operate and conduct themselves in a way that is compliant with financial services industry requirements so that the Director can be assured that those staff are aware of their legal and regulatory	
PPCL2-RC-006		PPCL1-006	#########	Compliance	The supplier shall ensure that any data is captured, processed, hosted and stored in accordance with relevant data protection legislation and the Director's customer data retention rules.	
PPCL2-INT-001		PPCL1-010	#########	Competitor, Service and Customer	The Supplier shall ensure access to, creation and amendment of the appropriate customer data, so that the Director can provide the required tailored service to all customers, as needed	
PPCL2-INT-002		PPCL1-010	#########	Competitor, Service and Customer	The Supplier's solution shall integrate data and insight with other parts of the wider Directors ecosystem, so that the Director can ensure delivery and continuous improvement of all its services	
PPCL2-INT-003		PPCL1-010	#########	Competitor, Service and Customer	The Supplier's solution shall provide actionable insight regarding customer experience and operations of the service, to a cadence agreed with the Director, so that the Director and other Suppliers are able to understand the underlying cause of issues and continuously improve	
PPCL2-INT-004		PPCL1-010	#########	Competitor, Service and Customer	The supplier's solution shall enable access to operational data, so that the Director and its suppliers can assess and improve operational effectiveness of services provided within the procurement package.	
PPCL2-INT-005		PPCL1-010	#########	Competitor, Service and Customer	The Supplier shall provide customer journey recommendations for all Supplier provisioned services, so that the Directors customer experience can be continuously improved across all services	
PPCL2-INT-006		PPCL1-010	#########	Competitor, Service and Customer	The supplier shall create and manage data according to the Director's Data Governance standards, processes and forums so that the provisioned data and any actionable insight can be relied upon by the Directors organisation	
PPCL2-TRF-001		PPCL1-011	#########	Transformation	The supplier shall deliver, for Director agreement, and then execute against a strategy to appropriately drive customers to use the digital self serve-service, so that the Director can be assured of a strategy and delivery against that strategy, that achieves a transformational move to digital customer	The supplier shall demonstrate how they will help to drive the customers to use the digital self serve-service, so that the Director has a clear understanding of the journey from current state to the future operating model.
PPCL2-FC-001		PPCL1-012	#########	Financial Crime	The Supplier shall assure that business rules, controls and configuration changes are defined and implemented so that they are aligning to the Directors risk appetite and policies	
PPCL2-FC-002		PPCL1-012	#########	Financial Crime	The Supplier shall make risk based decisions based on recent customer behaviour for the purposes of requiring enhanced customer authentication, informed by the full Directors data set so that account information is not handed to bad actors.	
PPCL2-FC-003		PPCL1-012	#########	Financial Crime	The Provider shall have controls in place to identify unauthorised insider access to or activity on customer accounts, and if any suspicious activity is defined, it is investigated with the finding reported to the Director, to ensure customer accounts are safeguarded.	
PPCL2-FC-004		PPCL1-012	#########	Financial Crime	The Supplier shall provide the ability to manage financial crime cases and investigations so that the Director minimises reputational damage and financial losses and the Director maintains legal compliance	
PPCL2-OPS-022		PPCL1-002	#########	Non-Digital Operational Processing	The Supplier shall apply the following principles, standards and aspirations associated to non-digital processing across its services and processes so that customer journeys can be completed with minimal customer and operational effort	
PPCL2-FC-005		PPCL1-012	#########	Financial Crime	The Supplier shall ensure and evidence the appropriate oversight of setting and maintenance of business rules, controls and configuration changes so that they are aligning to the Directors risk appetite and policies	
PPCL2-FC-006		PPCL1-012	#########	Financial Crime	The Supplier shall assure that business rules, controls and configuration changes are defined and implemented so that they are aligning to the Directors risk appetite and policies	
PPCL2-FC-007		PPCL1-012	#########	Financial Crime	The Supplier shall make risk based decisions based on recent customer behaviour for the purposes of requiring enhanced customer authentication, informed by the full Directors data set so that account information is not handed to bad actors.	
PPCL2-FC-008		PPCL1-012	#########	Financial Crime	The Provider shall have controls in place to identify unauthorised insider access to or activity on customer accounts, and if any suspicious activity is defined, it is investigated with the finding reported to the Director, to ensure customer accounts are safeguarded.	
PPCL2-FC-010		PPCL1-012	#########	Financial Crime	The supplier shall ensure appropriate staffing levels are in place to discharge the services of the Financial Crime function. Staff operational hours are to be agreed with the Director.	
PPCL2-FC-011		PPCL1-012	#########	Financial Crime	The supplier shall ensure the outsourced financial crime function is designed and operates in line with guidance from the UK's Joint Money Laundering Steering Group and the FCA Financial Crime Guide: A firm's guide to countering financial crime risks. The supplier shall ensure any future revisions of such guidance are adhered to and applied to the outsourced NS&I Financial Crime Function.	

L3 Requirement ID	Link to L2	Grouping	Requirement (incl. the 'what' and the 'why')	Previous Requirement
PPCL3-ART-001	PPCL2-ART-001	**Architecture**	The Supplier Solution shall integrate with other Supplier solutions, so that a seamless end-to-end supplier services are delivered.	
PPCL3-ART-002	PPCL2-ART-001	**Architecture**	The Supplier shall provide all of the software required to operate their solution in line with the other requirements, so that the supplier will provide managed services to Director.	
PPCL3-ART-003	PPCL2-ART-001	**Architecture**	The Supplier shall provide all of the personnel and skilled resources required to operate their solution in line with the other requirements, so that the supplier will provide managed end-to-end services to Director.	
PPCL3-ART-004	PPCL2-ART-001	**Architecture**	The Supplier shall provide all of the external services required to operate their solution in line with the other requirements, so that the supplier will provide managed end-to-end services to Director.	
PPCL3-ART-005	PPCL2-ART-001	**Architecture**	The Supplier shall remain responsible for any third party vendor, PaaS, SaaS or other cloud based service that it requires to run its solution, so that the solution will not require these resources from the Director.	
PPCL3-ART-006	PPCL2-ART-001	**Architecture**	The Supplier shall ensure that all infrastructure (hardware and software) is hardened and secured in a manner that is agreed with the Director, so that the infrastructure are properly protected.	
PPCL3-ART-007	PPCL2-ART-001	**Architecture**	The Supplier shall provide ongoing maintenance for their solution so that it maximised the availability, performance and security for customers	
PPCL3-ART-008	PPCL2-ART-001	**Architecture**	The Supplier shall provide continuous improvements to its delivered solution so that the overall customer experience and customer satisfaction improves over time.	
PPCL3-ART-009	PPCL2-ART-001	**Architecture**	The Suppliers solution shall maintain versions of the solution's components and services at mainstream supported levels, so that Director's services will have mainstream maintenance in line with the market.	
PPCL3-ART-010	PPCL2-ART-001	**Architecture**	The Supplier shall maintain a horizon scanning function that identifies and prioritises (in conjunction with the Director) the deployment of vendor software patches	
PPCL3-ART-011	PPCL2-ART-001	**Architecture**	The Supplier shall report out to the Service Management Toolset (e.g. Service Now) the patching levels of their services, including any outstanding patches (including those which have been chosen not to be applied), so that Director will be aware of the completeness of patches.	
PPCL3-ART-012	PPCL2-ART-001	**Architecture**	The Supplier shall provide system administration and control functions for managing their solution, so that Director's services will be managed efficiently.	
PPCL3-ART-013	PPCL2-ART-001	**Architecture**	The Suppliers solution shall maintain the availability, confidentiality and integrity of all information it has received and manages for the purposes of delivering its services	
PPCL3-ART-014	PPCL2-ART-001	**Architecture**	The Supplier shall provide the tools, knowledge and assistance so that the supplier themselves and the Director can create and edit content to support the customer services.	
PPCL3-ART-015	PPCL2-ART-001	**Architecture**	The Supplier shall collaborate with Other Suppliers, including the incumbent Supplier, so that integration across the Transition States is supported and aligned. Collaboration activities include but are not limited to: availability of resources (e.g. latest designs), knowledge transfer.	
PPCL3-ART-016	PPCL2-ART-001	**Architecture**	The Supplier shall provide the Director with information of non-compliance to Enterprise Architecture approved designs and standards which have been identified during integration of other Supplier solutions, so that the Director can appropriately mitigate against any risks of non-compliance or mis-alignment.	
PPCL3-ART-017	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that their solution is modular by design, so that modules, components and functionality can be compartmentalised and reused by the Director so that interdependencies are reduced	
PPCL3-ART-018	PPCL2-ART-003	**Architecture**	The Supplier shall ensure the architecture for the provided solution is open and extensible, so that the Director is able to evolve its business capabilities and services as required	
PPCL3-ART-019	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that their solution is a loosely coupled design, so that there is simplified integration with other solutions, services and technologies	
PPCL3-ART-020	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that modules or integrations with external services are loosely coupled, so that that they can be updated or replaced with minimal impact on the entire provisioned solution	
PPCL3-ART-021	PPCL2-ART-003	**Architecture**	The Suppliers solution shall allow for open or industry standards which are not proprietary to the service provider, including alignment with open standards/principles and API industry guidelines issued by the Government Digital Service (GDS) as well as those specified in the Director's Rainbow GDS playbook, so that the Director is not bound by technology provided by specific providers.	
PPCL3-ART-022	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that all technical interface design follows the Guidance and Technology Code of Practice of the UK Government, so that the Director's system services can be integrated with other solutions effectively.	
PPCL3-ART-023	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that all technical interfaces enforce mutual authentication wherever possible, so that both client and server can be verified and trusted	
PPCL3-ART-024	PPCL2-ART-003	**Architecture**	The Supplier shall agree with the Director for any technical interfaces that does not use mutual authentication, so that the interface communication meets specific technical or business needs.	
PPCL3-ART-025	PPCL2-ART-003	**Architecture**	The Supplier shall ensure that any technical interface version upgrade is backward compatible with the previous versions wherever possible, so that the Director's full end-to-end services can be maintained during transition.	
PPCL3-ART-026	PPCL2-ART-003	**Architecture**	The Supplier shall ensure flexible release mechanisms are adopted, so that Other Suppliers can upgrade to the use of the new technical interface version at a later date, so that the Director's full end-to-end services can be maintained during transition.	
PPCL3-ART-027	PPCL2-ART-003	**Architecture**	The Supplier shall develop and provide a high-level technical roadmap for their solution which is initially aligned to the four Transition States and subsequently covers the full length of Package C, so that the Director has visibility of future alignment with the Director's Enterprise Architecture strategy. Information within the technical roadmap to include but is not limited to: *Planned released / release dates *Key features to be included	
PPCL3-ART-028	PPCL2-ART-004	**Architecture**	The Supplier shall use the Directors preferred integration approaches, where specified, so that the Director can have an integrated and decoupled suite of services	
PPCL3-ART-029	PPCL2-ART-004	**Architecture**	The Supplier shall implement preferred, as defined in the Directors High Level Design, tooling where possible, so that the Director can have an end-to-end view of the performance of the services	
PPCL3-ART-030	PPCL2-ART-005	**Architecture**	The Supplier shall provide a customizable workflow that supports low-code business modelling and process automation with Director's other systems and solutions of Other Suppliers where appropriate, so that the Director's full end-to-end services can be delivered	
PPCL3-ART-031	PPCL2-ART-005	**Architecture**	The Supplier shall adapt their solution to the Directors changing estate of services, so that there is no disruption to the Directors continuous improvement	
PPCL3-ART-032	PPCL2-ART-005	**Architecture**	The Supplier shall design and implement the technical interfaces required for integration with Director's other systems and solutions of Other Suppliers, so that the Director's full end-to-end services can be delivered	
PPCL3-ART-033	PPCL2-ART-006	**Architecture**	The Supplier shall build in redundancy to their solution, so that it is free from single points of failure that could cause any part of the service to become unavailable.	
PPCL3-ART-034	PPCL2-ART-006	**Architecture**	The Supplier shall provide a solution that includes geo-graphical resilience of its components, so that the Director's services will not be impacted by interruptions in a single area.	
PPCL3-ART-035	PPCL2-ART-006	**Architecture**	The Supplier shall provide a monitoring capability to enable the automatic detection of system failures within the solution, so that the supplier and Director will be notified and take appropriate actions.	
PPCL3-ART-036	PPCL2-ART-006	**Architecture**	The Supplier shall ensure its solution provides the ability for administrators to modify settings, configuration and business rules without disrupting live services wherever possible, so that the Director's services can meet business needs.	
PPCL3-ART-037	PPCL2-ART-006	**Architecture**	The Supplier shall ensure that the deployment of new services or solutions will have minimal disruption to the business wherever possible, so that the Director's services can meet business needs.	
PPCL3-ART-038	PPCL2-ART-006	**Architecture**	The Supplier shall provide a solution designed to enable components of the solution to be upgraded or updated without causing disruption to the availability of its service wherever possible, so that the Director's services can meet business needs.	
PPCL3-ART-039	PPCL2-ART-006	**Architecture**	The Supplier shall provide a solution designed to enable maintenance to be performed without causing disruption or downtime to the availability of its service wherever possible , so that the Director's services can meet business needs.	
PPCL3-ART-040	PPCL2-ART-006	**Architecture**	The Supplier shall agree with the Director in advance of carrying out any administration or maintenance tasks that cause disruption to the service, and shall only carry these out within Authorised maintenance windows, so that the Director's services can meet business needs.	
PPCL3-ART-041	PPCL2-ART-006	**Architecture**	The Solution shall be capable to maintain service hours of 24x7x365, so that the Director's services can meet business needs.	
PPCL3-ART-042	PPCL2-ART-006	**Architecture**	The Supplier's solution shall be designed to be resilient to failures of third party or other connected systems, so that all other elements of the service it is providing remain functional.	
PPCL3-ART-043	PPCL2-ART-006	**Architecture (Disaster Recovery)**	The Supplier shall protect all data and recovery services from becoming unavailable during disaster events, so that Director can resume all business services.	

PPCL3-ART-044	PPCL2-ART-007	**Architecture**	The Supplier shall provide all of the compute capacity required to operate their solution in line with the performance, availability and scalability requirements, so that the Director's services can meet the business needs	
PPCL3-ART-045	PPCL2-ART-007	**Architecture**	The Supplier shall provide all of the networking required to operate their solution in line with the performance, availability and scalability requirements, so that the Director's services can meet the business needs	
PPCL3-ART-046	PPCL2-ART-007	**Architecture**	The Supplier shall provide all of the storage required to operate their solution in line with the performance, availability, data retention and scalability requirements, so that the Director's services can meet the business needs	
PPCL3-ART-047	PPCL2-ART-007	**Architecture**	The Supplier shall ensure that their solution is capable of scaling up dynamically to cope with sudden increase workload so that it is able to continue meeting the performance parameters supplied by the Director.	
PPCL3-ART-048	PPCL2-ART-007	**Architecture**	The Supplier shall ensure that their solution is capable of scaling down dynamically to reduce running costs when the experienced workload is reduced so that the solution continues meeting the performance parameters supplied by the Director cost effectively.	
PPCL3-ART-049	PPCL2-ART-020	**Architecture**	The Supplier shall provide data with complete accuracy at all states for active customer data, financial data and reporting data, so that the Director's service remains intact	
PPCL3-ART-050	PPCL2-ART-020	**Architecture**	The Supplier shall provide data which is as accurate as possible, so that the Director can optimise the services it delivers	
PPCL3-ART-051	PPCL2-ART-020	**Architecture**	The Supplier shall provide full data at rest integrity, so that the Director does not incur any reputational, financial or operational damage, and the Director remains compliant with GDPR	
PPCL3-ART-052	PPCL2-ART-020	**Architecture**	The Supplier shall provide full data in transit integrity, so that the Director does not incur any reputational, financial or operational damage, and the Director remains compliant with GDPR	
PPCL3-ART-053	PPCL2-ART-020	**Architecture**	The Supplier shall ensure that data integrity remains intact for encrypted and decrypted data, so that the Director does not incur any reputational, financial or operational damage, and the Director remains compliant with GDPR	
PPCL3-ART-054	PPCL2-ART-020	**Architecture**	The Supplier shall ensure that data is processed with full accuracy within all supplier provisioned services, so that Director can make and report the fully informed business decisions	
PPCL3-ART-055	PPCL2-ART-020	**Architecture**	The Supplier shall ensure that data is free from unauthorised access or changes, so that the Director does not incur any reputational, financial or operational damage, and the Director remains compliant with GDPR	
PPCL3-ART-056	PPCL2-ART-021	**Architecture**	The Supplier shall respect data rules set by Other Suppliers, so that the Director's data remains accurate and available across all (end-to-end) services	
PPCL3-ART-057	PPCL2-ART-021	**Architecture**	The Supplier shall respond and update when Other Suppliers request updates to the data hold/master data, so that the Director's data remains accurate and available across all services	
PPCL3-ART-058	PPCL2-ART-021	**Architecture**	The Supplier shall raise and report when data within Other Suppliers services is not accurate or breaches integrity, so that the Director's data remains accurate and available across all services	
PPCL3-ART-059	PPCL2-ART-021	**Architecture**	The Supplier shall issue requests to update data hold/master data with Other Suppliers when required, so that the Director's data remains accurate and available across all services	
PPCL3-ART-060	PPCL2-ART-021	**Architecture**	The Supplier shall collaborate with Other Suppliers and the Director to develop and update the data model and flows, so that the Director understands the responsibility of data during its end-to-end journey	
PPCL3-ART-061	PPCL2-ART-002	**Architecture**	The Supplier shall ensure that final versions of deployed code shall be held in escrow, with access provided to the Director, where application development is required; fresh versions of the code shall be deposited each time an update is made to the deployed code, so that the Director can access the latest deployed code version.	
PPCL3-ART-062	PPCL2-ART-002	**Architecture**	The Supplier shall provide a dedicated code repository in which to store all code developed by and for their solution, so that the Director can access code effectively.	
PPCL3-ART-063	PPCL2-ART-002	**Architecture**	The Supplier shall ensure that all interfaces and their functionality is fully documented such that the Director and Other Suppliers are able to interface to them without requiring supplier assistance, so that the Director's full end-to-end services can be delivered	
PPCL3-ART-064	PPCL2-ART-002	**Architecture**	The Supplier shall make available to the Director resources and documentation relevant to the Director's intellectual property, so that the Director has access to information required to run and maintain Solution being procured. Information and documentation includes but is not limited to: configurations used, code repository, design documentation, escrow arrangements	
PPCL3-ART-065	PPCL2-ART-009	**Architecture**	The Supplier shall operate the supplier services as a fully managed, to include the people, processes and technology so that the Directors business outcomes are achieved	
PPCL3-ART-066	PPCL2-ART-009	**Architecture**	The Supplier shall ensure that all changes made to the live environment are covered by effective change management processes, so that Director will be assured changes are deployed in a controlled and timely manner.	
PPCL3-ART-067	PPCL2-ART-009	**Architecture**	The Supplier shall ensure that their change management processes will interface with the Director's wider change management system, so that the Director has oversight across all suppliers to ensure schedule changes are compatible for the end-to-end service	
PPCL3-ART-068	PPCL2-ART-009	**Architecture**	The Supplier shall enable the Director to have the final say regarding when and what changes are implemented, so that the changes will be best fit the Director's needs.	
PPCL3-ART-069	PPCL2-ART-009	**Architecture**	The Supplier shall communicate upcoming changes with the Director and their other delivery partners, so that schedule changes are compatible for the end-to-end service	
PPCL3-ART-070	PPCL2-ART-009	**Architecture**	The Supplier shall coordinate and adhere to the Director and Other Suppliers as their solution will be delivered and improved incrementally over a number of transition states, so that schedule changes are compatible for the end-to-end solution.	
PPCL3-ART-071	PPCL2-ART-009	**Architecture**	The Supplier change management processes shall support the use of iterative delivery methods, so that some of the business value can be delivered earlier	
PPCL3-ART-072	PPCL2-ART-009	**Architecture**	The Supplier shall publish a forward schedule of change to proactively manage its product and service improvements, so that the Director can be assured of a continuous improvement approach being undertaken.	
PPCL3-ART-073	PPCL2-ART-009	**Architecture**	The Supplier shall provide a scalable team which is appropriately sized to carry out all planned and unplanned changes (including, but not limited to agile, continuous improvement and large-scale changes) in addition to the day-to-day operation of the solution, so that change is delivered efficiently and effectively	The Supplier shall provide a scalable team which is appropriately sized to carry out all changes, including continuous improvement and large-scale changes, in addition to the day to day operation of the solution, so that change management is appropriately resourced.
PPCL3-ART-074	PPCL2-ART-009	**Architecture**	The Supplier shall support the Director-driven business change of all sizes through the provision of technical resources, so that there is capacity and capability to embed change.	
PPCL3-ART-075	PPCL2-ART-009	**Architecture**	The Supplier shall provide a Change process which is aligned to the Director's Change process and Good Industry Practice standards, so that the Director has visibility over how the change lifecycle will be managed.	
PPCL3-ART-076	PPCL2-ART-009	**Architecture**	The Supplier shall follow a proactive change management framework which is overseen and governed by the Director, so that product / service updates and improvements are prioritised using the Director's prioritisation methods	
PPCL3-ART-077	PPCL2-ART-009	**Architecture**	The Supplier shall provide advance notice of any upgrades to external interfaces to Director and other Suppliers, so that upgrades are compatible for the end-to-end service.	
PPCL3-ART-078	PPCL2-ART-009	**Architecture**	The Supplier shall make available resources to support other Suppliers with any integration development and testing for the end to end solution, so that the end-to-end services can be delivered	
PPCL3-ART-079	PPCL2-ART-009	**Architecture**	The Supplier shall provide a representative development/test instance of any technical interfaces so that other Suppliers are able to develop and test integrations without impact live services	
PPCL3-ART-080	PPCL2-ART-009	**Architecture**	The Supplier shall provide advance notice of technical interface version upgrade to the Director and Other Suppliers, so that these suppliers have sufficient opportunity to ensure that upgrades are compatible and will not impact the delivery of the end-to-end service.	
PPCL3-ART-081	PPCL2-ART-009	**Architecture**	The Supplier shall provide all infrastructure (hardware and software) required to design, develop, test and run the supplier services without the need for any infrastructure from the Director so that the Supplier has control over the asset base	
PPCL3-ART-082	PPCL2-ART-009	**Architecture**	The Supplier shall remain responsible for all acts and omissions of its Sub-contractors and the acts and omissions of those employed or engaged by the Sub-contractors as well as contract, risk, performance and security related to any third party vendor, PaaS, SaaS or other cloud based service that it requires to run its solution so that the Supplier has control over the asset base	
PPCL3-ART-083	PPCL2-ART-010	**Architecture**	The Supplier shall ensure that effective change management processes are followed for all changes made to the live instance of their solution so that the changes are realised with suitable control and governance	
PPCL3-ART-084	PPCL2-ART-010	**Architecture**	The Supplier shall ensure all elements of their solution are fully tested and all functional requirements are met, so that Director's end-to-end services will work as expected.	
PPCL3-ART-085	PPCL2-ART-010	**Architecture**	The Supplier shall provide automated testing tools and evaluate the test output against predicted results, so that the testing is carried out efficiently.	
PPCL3-ART-086	PPCL2-ART-010	**Architecture**	The Supplier shall carry out integrated testing to ensure all system components work together and are free from error, so that end-to-end services can be provided.	
PPCL3-ART-087	PPCL2-ART-010	**Architecture**	The Supplier shall carry out quality assurance testing to ensure solution meet quality and reliability standards, so that Director's end-to-end services will work as expected.	

PPCL3-ART-088	PPCL2-ART-010	**Architecture**	The Supplier shall carry out loading and performance testing to ensure its solution's capacity and performance meets the requirements, so that Director's end-to-end services can meet the business demand.	
PPCL3-ART-089	PPCL2-ART-010	**Architecture**	The Supplier shall provide management functions to handle the setup and configuration of any required development and testing environments, so that development and testing environments will be managed efficiently.	
PPCL3-ART-090	PPCL2-ART-010	**Architecture**	The Supplier shall provide the tools necessary to automate the compilation and integrated testing of all developed code, so that integration test will be carried out efficiently.	
PPCL3-ART-091	PPCL2-ART-010	**Architecture**	The Supplier shall provide the tools necessary to automate the release of code to the code repository after successfully integration test, so that Director can access the tested code.	
PPCL3-ART-092	PPCL2-ART-010	**Architecture**	The Supplier shall provide appropriate tools and resources to manage all stages of the integrated testing and deployment pipeline from source code, building/compilation, testing through to deployment, so that the testing and deployment will be carried out effectively	
PPCL3-ART-093	PPCL2-ART-010	**Architecture**	The Supplier shall provide automatic notifications to users for any failure in the integrated testing and deployment pipeline, so that issues will be resolved in a timely manner.	
PPCL3-ART-094	PPCL2-ART-010	**Architecture**	The Supplier shall provide the tools to monitor integrated testing and deployment KPIs (such as cycle time, development frequency, change lead time, failure rate, mean time to recovery etc.), and improve where required, so that testing and deployment activities can be reviewed by the Director and the Supplier and improved.	
PPCL3-ART-095	PPCL2-ART-010	**Architecture**	The Supplier shall provide tools to automate the deployment of developed components to environments such as integration test, UAT, pre-production and production	
PPCL3-ART-096	PPCL2-ART-010	**Architecture**	The Supplier shall provide development environments that are separated from the live solution so that development and testing can be carried out with zero risk of disruption to customers	
PPCL3-ART-097	PPCL2-ART-010	**Architecture**	The Supplier shall ensure that their change management processes will interface with the Director's wider change management system so that the Director has oversight across all Suppliers to ensure schedule changes are compatible for the end-to-end service	
PPCL3-ART-098	PPCL2-ART-010	**Architecture**	The Supplier shall perform Horizon Scanning of emerging issues, risks and opportunities (e.g. emerging supplier provisioned service hygiene factors, legislation, and technologies), so that its roadmap aligns with the market and customer expectations.	
PPCL3-ART-099	PPCL2-ART-010	**Architecture**	The Supplier shall work with the Director to ensure that the Supplier's product roadmap and service development roadmap align so that the Director's planning capability is unhindered and the Director is able to reduce wasted efforted due to lack of alignment	The Supplier shall work with the Director to ensure that the Supplier's product roadmap and service development roadmap align so that the Director has unhindered planning capability and is able to reduce wasted efforted due to lack of alignment
PPCL3-ART-100	PPCL2-ART-010	**Architecture**	The Supplier shall provide one or more scalable teams for the specified services, appropriately sized to carry out all changes, including continuous improvement and large-scale changes, in addition to the day to day operation of Solution, so that change management is appropriately resourced.	
PPCL3-ART-101	PPCL2-ART-010	**Architecture**	The Supplier shall support the Director-driven business change of varying sizes and cadences through the provision of appropriate resources, so that there is capacity and capability to deliver change at the agreed pace.	
PPCL3-ART-102	PPCL2-ART-010	**Architecture**	The Supplier shall follow a change management framework which is overseen and governed by the Director, so that product / service updates and improvements are prioritised using the Director's prioritisation methods	
PPCL3-ART-103	PPCL2-ART-010	**Architecture**	The Supplier shall use independent testing to ensure that all products designed and developed by them are usable by people with disabilities (such as vision, hearing, mobility, thinking and understanding) and achieve Web Content Accessibility Guidelines WCAG 2.1 level AA so that our products are inclusive and accessible by default	
PPCL3-ART-104	PPCL2-ART-010	**Architecture**	The Supplier shall use independent testing to ensure that all products designed and developed by them are usable by people with disabilities (such as vision, hearing, mobility, thinking and understanding) and comply with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and the Equalities Act (2010) so that our products are inclusive and accessible by default	
PPCL3-ART-105	PPCL2-ART-010	**Architecture**	The Supplier shall use independent testing to ensure that all products designed and developed by them are usable by people with disabilities (such as vision, hearing, mobility, thinking and understanding) and work on the most commonly used assistive technologies, including but not limited to screen magnifiers, screen readers and speech recognition tools work effectively so that our products are inclusive and accessible by default.	
PPCL3-ART-106	PPCL2-ART-010	**Architecture**	The Supplier shall ensure that all products designed and developed by them are usable by people with disabilities (such as vision, hearing, mobility, thinking and understanding) and include disabled people in independent user research and testing so that real world testing is applied alongside simulations to ensure our products are inclusive and accessible by default.	
PPCL3-ART-107	PPCL2-ART-010	**Architecture**	The Supplier shall ensure that all products designed and developed by them are usable by people with disabilities (such as vision, hearing, mobility, thinking and understanding) and provide an accessibility audit by a 3rd party auditor so that their accessibility is independently verifiable	
PPCL3-ART-108	PPCL2-ART-010	**Architecture**	The Supplier shall ensure that all products are subjected to independent accessibility testing to ensure they comply with industry good practice as well as applicable laws and regulations so that any features, testing and claims are independently verifiable.	
PPCL3-ART-109	PPCL2-ART-010	**Architecture**	The Supplier shall provide all people, software and equipment required to carry out accessibility testing.	
PPCL3-ART-110	PPCL2-ART-010	**Architecture**	The Supplier shall ensure skills, equipment and software provided are industry recognised as being able to effectively be used for accessibility testing to the standards required by the regulations so that users can be assured that the mainstream accessibility tools will work effectively.	
PPCL3-ART-111	PPCL2-ART-012	**Architecture**	The Supplier shall work with the Director and Other Suppliers to migrate any required data into the new supplier solution so that the Directors operational continuity can be maintained	
PPCL3-ART-112	PPCL2-ART-012	**Architecture**	The Supplier shall work with the Director, and Other Suppliers to migrate email settings and mailboxes into the new Supplier solution, so that interaction can be maintained	
PPCL3-ART-113	PPCL2-ART-013	**Architecture**	The Supplier shall regularly monitor and report on the availability and health of their services to the Director and Other Suppliers, so that the Directors operations can be continued with minimised impediment	
PPCL3-ART-114	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all system applications within their sphere of responsibility and raise alerts to the Director and Other Suppliers when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-115	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all hosting devices and services within their sphere of responsibility and raise alerts to the Director and Other Suppliers when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-116	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all storage devices and services within their sphere of responsibility and raise alerts to the Director and Other Suppliers when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-117	PPCL2-ART-013	**Architecture**	The Supplier shall provide proactive monitoring network devices and services within their sphere of responsibility and raise alerts to the Director and Other Suppliers when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-118	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the health of system interfaces within their sphere of responsibility and raise alerts when to the Director and Other Suppliers events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-119	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor their ability to be able to use third party connected systems and raise alerts to the Director and Other Suppliers when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-120	PPCL2-ART-013	**Architecture**	The Supplier shall provide operational data to the Director's central SIAM function via the integration platform, so that the Director is able to have a true end to end view of the status of the services	
PPCL3-ART-121	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the availability of their provided solution and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-122	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the performance of their provided solution and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-123	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the functionality of their provided solution and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-124	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor their solution for unauthorised activity and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-125	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor their solution for vulnerabilities and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	

PPCL3-ART-126	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor their solution for potential attacks and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-127	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor log files from their solution to detect suspicious activity and raise alerts when events are detected or thresholds are breached, so that issues can be detected and resolved in a timely manner.	
PPCL3-ART-128	PPCL2-ART-013	**Architecture**	The Supplier's solution shall retain and securely store all data associated with monitoring - including (but not limited to) records of human analysis of incidents, response steps taken, system logs, events and alerts - for 3 years from its creation., so that the Director can access data and take appropriate actions when required.	
PPCL3-ART-129	PPCL2-ART-013	**Architecture**	The Supplier shall be responsible for providing their own internal IT service management function to monitor the operational status and remediate issues as they arise, so that the Director can be assured the solution and services are well managed.	
PPCL3-ART-130	PPCL2-ART-013	**Architecture**	The Supplier shall be responsible for providing their own internal security operations function to monitor the security status and remediate issues as they arise, so that the Director can be assured the solution operations are in line with the set out provisions.	
PPCL3-ART-131	PPCL2-ART-013	**Architecture**	The Supplier shall record and track all incidents and problems detected within their solution, so that the Director can access and review all incidents and problems.	
PPCL3-ART-132	PPCL2-ART-013	**Architecture**	The Supplier shall record the ongoing status of each incident and problem, so that the Director can be notified of the status of an incident and problem.	
PPCL3-ART-133	PPCL2-ART-013	**Architecture**	The Supplier shall record the root cause of each incident and problem, so that the Director can fully understand and be assured the problem will not reoccur.	
PPCL3-ART-134	PPCL2-ART-013	**Architecture**	The Supplier shall record the fix or remediation for each incident and problem, so that Director can be notified how an incident and problem is fixed.	
PPCL3-ART-135	PPCL2-ART-013	**Architecture**	The Supplier shall forward incidents and problem records to the Director's central SIAM function via the integration platform so that the Director is able to have a true end to end view of their services	
PPCL3-ART-136	PPCL2-ART-013	**Architecture**	The Supplier shall record and track all security incidents and vulnerabilities detected within their solution, so that the Director can be notified.	
PPCL3-ART-137	PPCL2-ART-013	**Architecture**	The Supplier shall record the ongoing status of each security incident and vulnerability, so that the Director can have the status of incident.	
PPCL3-ART-138	PPCL2-ART-013	**Architecture**	The Supplier shall record the fix or remediation for each security incident and vulnerability, so that the Director can be notified.	
PPCL3-ART-139	PPCL2-ART-013	**Architecture**	The Supplier shall forward security incidents and vulnerabilities to the Director's Central Security Monitoring Service (CSMS) function via the integration platform, so that the Director is able to have a true end to end view of their services	
PPCL3-ART-140	PPCL2-ART-013	**Architecture**	The Supplier's solution shall provide monitoring information to a level of detail sufficient to support and enable incident investigation and shall include (but not be limited to): -The date and time of the incident -The source of the incident -The reason that the incident occurred - Error messages generated - Details on the format/payload of message that caused the error , so that the support and investigation can be carried out in an effective manner.	
PPCL3-ART-141	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all system applications within their sphere of responsibility and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-142	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all hosting devices and services within their sphere of responsibility and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-143	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all storage devices and services within their sphere of responsibility and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-144	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the operational status of all network devices and services within their sphere of responsibility and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-145	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the health of system interfaces within their sphere of responsibility and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-146	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor their ability to be able to use third party connected systems and raise alerts when events are detected or thresholds are breached so that customer access to services remains available at all times.	
PPCL3-ART-147	PPCL2-ART-013	**Architecture**	The Supplier shall provide a dashboard to display the overall operational health of the Suppliers services, so that Director has visibility of its operations	
PPCL3-ART-148	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the availability of its provisioned services and raise alerts when events are detected or thresholds are breached, so that the Supplier can take the necessary action and the Director is informed of its operations	
PPCL3-ART-149	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the performance of its provisioned services and raise alerts when events are detected or thresholds are breached, so that the Supplier can take the necessary action and the Director is informed of its operations	
PPCL3-ART-150	PPCL2-ART-013	**Architecture**	The Supplier shall pro-actively monitor the functionality of its provisioned services and raise alerts when events are detected or thresholds are breached, so that the Supplier can take the necessary action and the Director is informed of its operations	
PPCL3-ART-151	PPCL2-ART-013	**Architecture**	The Supplier shall provide a feed of provisioned services analytics data into the Knowledge and Insights capability so that the Director has a full analytical landscape of its services	
PPCL3-ART-152	PPCL2-ART-013	**Architecture**	The Supplier shall work collaboratively with Other Suppliers to design and implement the integration for passing analytics data to Other Suppliers and the Director, so that the Director has a full analytical landscape of its services	
PPCL3-ART-153	PPCL2-ART-013	**Architecture**	The Supplier solution shall be monitored on a 24x7x365 basis, so that the Supplier can identify and address any issues and the Director is informed about the status of their operations	
PPCL3-ART-154	PPCL2-ART-014	**Architecture**	The Supplier shall support the Director in improving the supplier provisioned services in line with emerging hygiene factors, as evidenced by Good Industry Practice, so that the Director can maintain the fast follower status	
PPCL3-ART-155	PPCL2-ART-014	**Architecture**	The Supplier shall provide regular insights into the development of the Supplier's product roadmap so that Solution is actively developed, and the roadmap aligns with the Director's strategic vision and Continuous Improvement Plan	
PPCL3-ART-156	PPCL2-ART-014	**Architecture**	The Supplier shall proactively propose roadmap enhancements relevant to the Director so that benefits from roadmap developments that improve customer and business outcomes can be identified e.g. cost-effectiveness, enhanced customer offer, and more rapid pace of change	
PPCL3-ART-157	PPCL2-ART-014	**Architecture**	The Supplier shall collaborate with the Director to plan relevant roadmap adoptions so that there is an agreed plan for maintaining alignment of the joint roadmap	
PPCL3-ART-158	PPCL2-ART-015	**Architecture**	The Supplier shall allow for regular reviews of upcoming developments and changes to all the product roadmaps, so that the Director can perform customer, market, and competitor analysis to understand when and whether to adopt roadmap developments	
PPCL3-ART-159	PPCL2-ART-018	**Architecture**	The Supplier shall provide data on operational delivery, so that the data can be blended with that from the Director and Other Suppliers, to develop further Actionable Insight	
PPCL3-ART-160	PPCL2-ART-018	**Architecture**	The Supplier shall provide data on service performance, so that the data can be blended with that from the Director and Other Suppliers, to develop further Actionable Insight	
PPCL3-ART-161	PPCL2-ART-018	**Architecture**	The Supplier shall provide insight into the potential positive and negative impacts of proposed changes so that the potential business and customer benefits of changes are assessed and prioritised accordingly	
PPCL3-ART-162	PPCL2-ART-018	**Architecture**	The Supplier shall provide management information on the Supplier's performance against KPIs, and PI's, so that the services and operations can be tracked, managed and improved	
PPCL3-ART-163	PPCL2-ART-008	**Architecture**	The Supplier shall provide all infrastructure (hardware and software) required to design, develop, test and run their solution so that the supplier will not require infrastructure from the Director.	
PPCL3-ART-164	PPCL2-ART-008	**Architecture**	The Supplier shall ensure that all hardware used in their solution remains in support with the manufacturer, so that the hardware will be under proper maintenance.	
PPCL3-ART-165	PPCL2-ART-008	**Architecture**	The Supplier shall ensure that software is patched and kept current, so that the software is in line with the Directors governance standards	
PPCL3-ART-166	PPCL2-ART-016	**Architecture**	The Supplier shall provide intelligence data and insights of their solutions within agreed time frame so that the Director can have services improvement recommendations and make decisions in a timely manner	
PPCL3-ART-167	PPCL2-ART-016	**Architecture**	The Supplier shall collaborate with Other Suppliers and provide intelligence data which can be combined with intelligence data from across the Enterprise, so that the Director can have complete view of cross business areas insights.	
PPCL3-ART-168	PPCL2-ART-019	**Architecture**	The Supplier shall maintain version control of their solution's components so that the Directors can access the required version in a timely manner.	
PPCL3-ART-169	PPCL2-ART-019	**Architecture**	The Supplier shall provide appropriate tools and processes to enable effective version control of all binary code in a repository, so that the Director can access a particular version of binary code when required.	

PPCL3-AD-001	PPCL2-AD-001	**Assisted Digital**	The Supplier shall provide documentation of operational processes and procedures (including people, technology, data etc) and how they are delivered so that the processes involved are understood and can be documented in the Director's architectural model and aligned to the Civil Service standard and the Director retains an understanding of how the services are delivered	
PPCL3-AD-002	PPCL2-AD-001	**Assisted Digital**	The Supplier shall respond to ad-hoc requests for management information so that the Director's stakeholders' (e.g. HM Treasury) reporting requirements are met	
PPCL3-AD-003	PPCL2-AD-001	**Assisted Digital**	The Supplier shall track and report on the progress of any recovery plans as required, so that the Director is informed of progress against plans and can manage stakeholders effectively.	
PPCL3-AD-004	PPCL2-AD-001	**Assisted Digital**	The Supplier shall, where applicable to individual service requirements and scope, support and/or deliver the following activities including but not limited to: ▪ Assurance and oversight activity; ▪ Complaints procedures & complaints handling; ▪ Analytics and Insights; ▪ Freedom of Information requirements; ▪ Subject Access Requests; ▪ Fraud/suspicious activity prevention and reporting; ▪ Auditing check and assessments; ▪ Change Request management and implementation; ▪ Contract Management; ▪ Training; ▪ Incident reporting and resolution; ▪ Resolution planning; and ▪ Issue identification, root cause analysis, escalation and remediation.	
PPCL3-AD-005	PPCL2-AD-001	**Assisted Digital**	Suppliers shall provide flexible and scalable contact centre and assisted digital capabilities so that it is in line with the ongoing demands of the Director	
PPCL3-AD-006	PPCL2-AD-001	**Assisted Digital**	The Supplier shall have the capability to provide a Scalable, resilient service, including physical contact centres and seat numbers, in the UK, as requested by the Director so that the Supplier is able to adapt to changes in products, strategic changes and external impacting factors.	
PPCL3-AD-007	PPCL2-AD-001	**Assisted Digital**	Supplier shall enable change in the event that Government standards changes from CCA to another accredited body or other arrangements so that the service remains compliant and aligned to best practice.	
PPCL3-AD-008	PPCL2-AD-001	**Assisted Digital**	The Supplier shall be responsible for providing the infrastructure required to support the delivery of the Services unless, otherwise specified by the Director, including but not limited to, networks, telephony and IT hosting architecture, and end user equipment.	
PPCL3-AD-009	PPCL2-AD-001	**Assisted Digital**	The Supplier shall provide all software and systems as required to deliver the services specified by the Director, including but not limited to, technical interfaces to other Suppliers services so that the Supplier is able to integrate its services with the Director and other Suppliers	
PPCL3-AD-010	PPCL2-AD-001	**Assisted Digital**	The Supplier shall provide an integrated and intuitive Agent interface so that agents are able to efficiently operate and are able to complete to resolve Customer journeys at first contact	
PPCL3-AD-011	PPCL2-AD-001	**Assisted Digital**	The Supplier shall provide a flexible approach to accommodation or home-working facilities that meets all legislative and Director's requirements so that there is the ability to scale up or down, in line with forecasts, activity levels, unforeseen events and security requirements.	
PPCL3-AD-012	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that the Contact Centre(s) are/is UK based so that the contact centre is staffed by UK based agents aligning to the government guidance	
PPCL3-AD-013	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that all processes to enable successful interactions with all Customer Personas in place and up to date in line with the Suppliers needs so that Customers can complete their journeys	
PPCL3-AD-014	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that any data that is stored or destroyed throughout the duration of contract, is done so in line with the Directors retention schedule so that the Director is compliant with the necessary legal requirements and regulatory standards.	
PPCL3-AD-015	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that any technical issues or Customer impacting incidents identified by Customers or agents are raised with the appropriate IT Help Desk so they can be investigated appropriately, communicated and resolved in a timely manner.	
PPCL3-AD-016	PPCL2-AD-001	**Assisted Digital**	The Supplier shall continually review, report and feedback on the service delivered to ensure they are providing the optimal Service so that it meets the Directors assurance requirement.	
PPCL3-AD-017	PPCL2-AD-002	**Assisted Digital**	The Supplier shall enable a contact centre agent to provide assistance to Customers so that Customers are supported to complete their 'jobs to be done'	
PPCL3-AD-018	PPCL2-AD-002	**Assisted Digital**	The Supplier shall provide Agents with the tools required to support continuation of digital Customer journey and progress to next steps so that the agent is able to provide the Customer with a Seamless Customer Experience.	
PPCL3-AD-019	PPCL2-AD-002	**Assisted Digital**	The Supplier shall enable Contact Centre Agents to restart or resume the Customer journey, so that the Agent can assist the Customer while speaking with them	
PPCL3-AD-020	PPCL2-AD-002	**Assisted Digital**	The Supplier shall design Customer journeys and experiences which can be quickly and easily adapted to better assist the Customer, so that Agents can rapidly enable Assisted Digital support	
PPCL3-AD-021	PPCL2-AD-002	**Assisted Digital**	The Supplier shall encourage Customers to digitally self serve their information and transactions and go paperless (e.g. setting up standing orders) so that Customers can complete their jobs to be done quickly and more efficiently.	
PPCL3-AD-022	PPCL2-AD-002	**Assisted Digital**	The Supplier shall design, test and deliver the required Help Content and Assisted Digital-related content (for the Customer and Agent), so that Customers are supported in achieving their Jobs to be Done on a continuous basis.	
PPCL3-AD-023	PPCL2-AD-002	**Assisted Digital**	The Supplier shall ensure that information and data from other Suppliers is quickly available to support the Agent and Customer to progress to next steps so that the Customer is able to quickly and efficiently complete their jobs to be done	
PPCL3-AD-024	PPCL2-AD-002	**Assisted Digital**	The Supplier shall design and implement a process which enables all Customer Personas contacting on behalf of Customers to be assisted by Agents so that Customers jobs are done via their proxy in a timely and efficient manner.	
PPCL3-AD-025	PPCL2-AD-003	**Assisted Digital**	The Supplier shall complete the end-to-end journey on the Customers behalf when instructed to do so by an authenticated Customer so that the Agent finishes the job to be done at first contact.	
PPCL3-AD-026	PPCL2-AD-003	**Assisted Digital**	The Supplier shall intervene to complete partially executed Customer journeys at any point on the Customers behalf when instructed to do so by an authenticated Customer, so that the Agent is able to resolve Customer journeys at first contact (dependent on capability to pause and resume journeys being delivered by other service delivery partners and the Directors desire to implement the service solution)	The Supplier shall intervene to complete partially executed Customer journeys at any point on the Customers behalf when instructed to do so by an authenticated Customer so that the Agent is able to resolve Customer journeys at first contact
PPCL3-AD-027	PPCL2-AD-003	**Assisted Digital**	The solution shall enable Contact Centre Agents to restart and resume the Customer journey, so that the Agent can undertake it on the Customer's behalf while speaking with them	
PPCL3-AD-028	PPCL2-AD-003	**Assisted Digital**	The Supplier shall design Customer journeys and experiences which allow agents to step in and efficiently operate on behalf of Customers, so that Agents can rapidly enable Assisted Digital support	
PPCL3-AD-029	PPCL2-AD-003	**Assisted Digital**	The Supplier shall design, test and deliver the required Help Content and Assisted Digital-related content (for the Customer and Agent), so that the Agent is able to carry out jobs to be done in a consistent basis.	
PPCL3-AD-030	PPCL2-AD-003	**Assisted Digital**	The Supplier shall encourage Customers to digitally self serve their information and transactions and go paperless (e.g. setting up standing orders) by demonstrating how to complete the process so that the Customer is informed on how to complete Customer transactions in the future and reduce the number of transactions where an Agent carries out Customer transactions on their behalf where possible.	
PPCL3-AD-031	PPCL2-AD-003	**Assisted Digital**	The Supplier shall ensure that the Agent has full access to Co-Browsing and video capability so that the Agent can carry out its required services to assist the Customer and complete transactions on their behalf.	
PPCL3-AD-032	PPCL2-AD-003	**Assisted Digital**	The Supplier shall ensure that the Agents scripts are designed to encourage Customers to digitally self serve where possible so that Customers increase the number of digital self serve transactions.	
PPCL3-AD-033	PPCL2-AD-003	**Assisted Digital**	The Supplier shall ensure that Agents are trained to encourage Customers to Digitally self serve (including through design of scripts) through available channels (e.g. cobrowsing) so that more Customers transition to digital self-service	
PPCL3-AD-034	PPCL2-AD-003	**Assisted Digital**	The Supplier shall design and implement a process which enables all Customer personas contacting on behalf of Customers for Agents to be able to complete jobs on the proxies behalf in a timely and efficient manner.	
PPCL3-AD-035	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure that agents have the capability to identify Customer vulnerability, either when the Agent is able to identify a Customer is vulnerable or the Customer voluntarily tells the Agent, so that the business is able to best serve the Customers needs	
PPCL3-AD-036	PPCL2-AD-004	**Assisted Digital**	'The Supplier shall ensure that vulnerable Customers are supported according to their particular vulnerabilities, so that the Directors obligations under the Equality Act 2010: Public sector equality duty, are met'	
PPCL3-AD-037	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure that vulnerable Customers should be proactively and consistently flagged to Agents across appropriate channels so that they can identify and service them in an appropriate and compliant way	
PPCL3-AD-038	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure that Agents are able to see any vulnerability data previously stored against a Customer's records, regardless of channel, so that the Customer has seamless Customer experience	

PPCL3-AD-039	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure the agents can capture and update into the retained Customer records data that a Customer is vulnerable and the nature of the vulnerability (e.g. permanent or temporary) aligned to the GDS and FCA guidance using life-stage categories so that the agent is able to ensure that Customer Records are kept up to date	
PPCL3-AD-040	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure that special category personal data is not transmitted in an unsecure environment so that the Director remains compliant	
PPCL3-AD-041	PPCL2-AD-004	**Assisted Digital**	The Supplier shall ensure that Customer marketing preferences are captured which encourages Customers to use one of the available digital channels and opts for digital communications so that the business increases the number of digital transactions	
PPCL3-AD-042	PPCL2-AD-004	**Assisted Digital**	The Supplier shall be able to access existing Customer data and preferences so that the agent is able determine the appropriate communication types, content and channels for a given Customer.	
PPCL3-AD-043	PPCL2-AD-004	**Assisted Digital**	The Supplier shall collect and manage the Customer consent to be contacted/or receive notifications and through which channels so that Agents ensure that the Customer is able to determine what information is captured about them	
PPCL3-AD-044	PPCL2-AD-005	**Assisted Digital**	The Supplier shall provide uninterrupted, continuous support where a Customer switches channels and/or devices within the agreed range so that Customers can be assisted in their interactions with the Director when using their preferred channel or switching between.	
PPCL3-AD-045	PPCL2-AD-005	**Assisted Digital**	The Supplier shall provide the Assisted Digital Support where Customers who use an agreed range of Devices (where Device means the combination of platform, OS, and/or browser) for each digital channel so that Customers can receive support when using their preferred device	
PPCL3-AD-046	PPCL2-AD-005	**Assisted Digital**	The Supplier shall provide consistency in service and support regardless of Customer's chosen channel(s) or device(s) so that the Assisted Digital support provides a consistent experience regardless of channel/device.	
PPCL3-AD-047	PPCL2-AD-005	**Assisted Digital**	The Supplier shall collaborate with the Director to apply consistent signposting and acknowledgement content within and across channels so that Customers are assured of the journey and its outcomes, reducing operational fallout.	
PPCL3-AD-048	PPCL2-AD-005	**Assisted Digital**	The Supplier shall work collaboratively with the Director and Other Suppliers to ensure that all required communication channels (email, SMS, push notifications, chat, secure messaging) are available and supported so that the Customer experiences a seamless Customer journey and included branded according to brand standards	
PPCL3-AD-049	PPCL2-AD-005	**Assisted Digital**	The Supplier shall be able to intuitively optimise Customer interactions to help drive continuous improvement so that the Service can continually improve its Customer experience.	
PPCL3-AD-050	PPCL2-AD-006	**Assisted Digital**	Suppliers shall proactively make recommendations on innovations from their horizon scanning, technical and market knowledge so that the Director is able to follow fast-follower status harnessing new technology and methods to provide innovations to give Customers improved Customer experience.	
PPCL3-AD-051	PPCL2-AD-006	**Assisted Digital**	The Supplier shall work in collaboration with the Director and Other Suppliers to explore possibilities for innovative technologies to further develop and enhance existing solutions so that the business is able to improve Customer experience	
PPCL3-AD-052	PPCL2-AD-006	**Assisted Digital**	The Supplier shall include the ability to explore technological/innovative solutions to handle interactions with the Customer so that it supports driving efficiencies and Customer satisfaction.	
PPCL3-AD-053	PPCL2-AD-006	**Assisted Digital**	The Supplier shall have the ability to explore technological/innovative solutions to handle interactions with the Customer so that the Service is able to help drive efficiency and positive Customer interactions.	
PPCL3-AD-054	PPCL2-AD-006	**Assisted Digital**	The Supplier's solution shall be future-proof to enable cost-effective, rapid addition and decommissioning of channel so that the business can deliver a seamless Customer experience without negatively impacting the Customer experience.	
PPCL3-AD-055	PPCL2-AD-007	**Assisted Digital**	The Supplier shall provide all necessary telephony services, including, but not limited to; -Communications technology (infrastructure, hardware, software) -Data analytics, Reporting and Performance Monitoring (real-time and historic) -Human resources (agents, management, support staff, recruitment, training, payroll, forecasting and planning) So that the operation demands of the Director are met	
PPCL3-AD-056	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure there is an AI voice solution within the IVR/Voice Assistant that understands natural language so that the Virtual Agent can converse with Customers to deal with Customer enquiries and transactions.	
PPCL3-AD-057	PPCL2-AD-007	**Assisted Digital**	The supplier shall leverage the strategic solution for customer authentication provided by the Digital Experience and Digital Enablement package supplier so that the risk engine has 360 degree visibility of customer authentication activity across all channels	The Supplier must leverage the strategic solution for authentication provided by other Suppliers so that the Customer maintains a seamless and consistent Customer journey.
PPCL3-AD-058	PPCL2-AD-007	**Assisted Digital**	The Supplier shall instruct Agents to encourage Customers towards digital self-serving information, transactions and paperless communications so that call volumes are reduced	
PPCL3-AD-059	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that all contact centre telephone numbers are retained and are freephone so that the Director's Customers expectations are met.	
PPCL3-AD-060	PPCL2-AD-007	**Assisted Digital**	The Supplier shall enable self-service through voice assistant/IVR where Customers can authenticate themselves so that the Customers can undertake various transactions including but not limited to; making a purchase, make a repayment, check a balance, change nominated bank details without the need to speak to an agent.	
PPCL3-AD-061	PPCL2-AD-007	**Assisted Digital**	The Supplier shall create an IVR/Voice Assistant prize checker capability where Customers can check their most recent and historical prizes via the IVR/Voice Assistant so that Customers can check the results quickly and easily without talking to the contact centre agent	
PPCL3-AD-062	PPCL2-AD-007	**Assisted Digital**	The Supplier shall provide a consistent Customer and brand experience, in collaboration with other Suppliers, when using the Prize Checker Service via the IVR/Voice Assistant capability so that they have a similar and identifiable feel, regardless of touchpoint	
PPCL3-AD-063	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that a customer can check historical Prize Draw results through the phone or other non-digital , if not able to through a digital channel, so that all digitally excluded or vulnerable customers are inclusive of the Prize Draw process	
PPCL3-AD-064	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that the financial advisor helpline telephone number is retained so that the business can maintain its current service	
PPCL3-AD-065	PPCL2-AD-008	**Assisted Digital**	The Supplier shall provide a secure messaging, agent chat and automated chat solution which; -provides a seamless transition between automated and agent chat -provides consistency in its look and feel across all channels in line with the Directors brand principles -uses consistent language and content across channels -adheres to response times as determined within the contract terms This is so that the business maintains a seamless and secure Customer experience.	
PPCL3-AD-066	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure where an AI solution is unable to answer a Customer query that the Supplier will enable the conversation to be handled by an Agent so that Agent can resolve the query	
PPCL3-AD-067	PPCL2-AD-008	**Assisted Digital**	The Supplier will ensure that agents focus on the quality of their responses and do not have more than three concurrent chats running so they are able to cope with the volume of chats and that the response is of a high standard.	
PPCL3-AD-068	PPCL2-AD-008	**Assisted Digital**	The Supplier shall create a process with clear rules for an agent using chat with the Customer including; -Training (or retraining where necessary) for the Agent be able to competently chat with the Customer -Guidance and prompts on when the Agent should suggest, at the most appropriate points, when to move to a different channel or Co-Browse (agents discretion) -Identifying any issues to help determine support required to unblock Customer journeys	
PPCL3-AD-069	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that secure messaging and chat capability is compatible with other Suppliers capability development so that the Customer is able to use the full chat capability to securely support completing their jobs to be done with the agent	
PPCL3-AD-070	PPCL2-AD-008	**Assisted Digital**	The Supplier shall enable the capability for a contact centre agent to pick up the message chat conversation from the chatbot and continue the conversation with a Customer so that the Customer has a positive interaction	
PPCL3-AD-071	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that the chat solution shall not require the Customer to download and install software onto their device so that the Customer journey is seamless	
PPCL3-AD-072	PPCL2-AD-008	**Assisted Digital**	The Supplier shall enable the mechanism for the Customer to either give clear and informed consent, or to reject the use of the chat feature with a contact centre agent so that the Customer is given autonomy on how they complete their Customer journey.	
PPCL3-AD-073	PPCL2-AD-008	**Assisted Digital**	The Supplier shall redact any sensitive data a Customer may have provided so that the data cannot be seen after the conversation has ended	
PPCL3-AD-074	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that no sensitive data is stored at the server side of the chat session so that Customers data is protected and the business is compliant	

PPCL3-AD-075	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that all chat sessions are recorded so that the sessions can be reviewed for training and quality purposes and ensure that actions taken by the Agent are to the highest standard to ensure the Customer receives the best possible experience	
PPCL3-AD-076	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that all recorded chat sessions are deleted aligned to the retention schedule so that the business is compliant	
PPCL3-AD-077	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that email is available where it is required and for any other additional processes including, but not limited to; -Complaint, -FOI and -Data Subject This is so that the business remains compliant and is able to deal with correspondence in an effective and secure way	
PPCL3-AD-078	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that the contact centre is available 24/7 for 366 days per year for the Chatbot so that Customers have optimal access to the contact centre	
PPCL3-AD-079	PPCL2-AD-008	**Assisted Digital**	The Supplier will ensure Customers are able to converse with a chat agent during the hours specified/agreed with the Director	
PPCL3-AD-080	PPCL2-AD-008	**Assisted Digital**	The Supplier will ensure Customers are able to converse with a chat agent during the same hours as the phone channel is available so that there is a consistent approach.	
PPCL3-AD-081	PPCL2-AD-009	**Assisted Digital**	The Supplier shall ensure that they have the capability to facilitate calls from Other Suppliers' applications "in-app call" features so that the Director can complete customer journeys from all possible channels	
PPCL3-AD-090	PPCL2-AD-012	**Assisted Digital**	The Supplier will meet the Directors defined performance indicators, including but not limited to, speed to answer/respond, CSAT, accuracy and abandoned rate so the Director can achieve the operational performance targets.	
PPCL3-AD-091	PPCL2-AD-012	**Assisted Digital**	The Supplier shall have a quality improvement strategy and be able to demonstrate to the Director how this mechanism operates and be able to share the outputs with the Director so that the assurance and oversight needs of the Director are met	
PPCL3-AD-092	PPCL2-AD-012	**Assisted Digital**	The Supplier shall provide a highly performing contact recording system that records all contacts that are presented within the contact centre and that these contacts are available for a period aligned to the Directors retention schedule so that the business is able to review contact quality and provide recorded contacts where required	
PPCL3-AD-093	PPCL2-AD-012	**Assisted Digital**	The Supplier shall ensure the Director has access to the necessary systems so that the Director has clear independent visibility of all contacts and performance MI (real-time and historical), reasons for contact and can assure the service.	
PPCL3-AD-094	PPCL2-AD-013	**Assisted Digital**	The Supplier shall empower their agents with the information, technology and soft skills so that the agents can complete the Customer journey and exceed Customer expectations at the first point of contact	
PPCL3-AD-095	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide the recruitment, management and development of all appropriately skilled staff required for the delivery of the Directors operations across all contact channels.	
PPCL3-AD-096	PPCL2-AD-013	**Assisted Digital**	The Supplier shall have provisions in place to support the retention of staff and knowledge so that consistent levels of service are maintained including; -Performance of resource -Commercial agreement -Cultural mindset for first contact resolution (% for first contact resolution completion) and; -Encourage digital self-service (digital nudges)	
PPCL3-AD-097	PPCL2-AD-013	**Assisted Digital**	The Supplier will ensure any agents being onboarded to respond to all communications are pre-screened in the recruitment process to ensure they have an excellent command of the English language including spelling, grammar and tone so that agents are able to clearly communicate with Customers	
PPCL3-AD-098	PPCL2-AD-013	**Assisted Digital**	The Supplier shall ensure that Agents are fully trained so that Agents are able to operate in a compliant (and effective way. This includes but is not limited to; -Systems Training -Product Knowledge -Soft Skills -Technical Queries (Website & App trouble shooting) -Digital Nudging	
PPCL3-AD-099	PPCL2-AD-013	**Assisted Digital**	The Supplier will ensure all agents responding to online related enquiries and have a good, sound knowledge of the online content, functionality and processes which underpin it so that they are able to respond to the Customers enquiry quickly and with the correct information.	
PPCL3-AD-100	PPCL2-AD-013	**Assisted Digital**	The Supplier shall ensure that the Director has sight of training plans and at request the ability to input to training material so that the business remains compliant and Agents operate to a high standard.	
PPCL3-AD-101	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide the Director with opportunity to attend training sessions so that the Director is able to assure the training being delivered is fit for purpose	
PPCL3-AD-102	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide training progress reports to the Director so that the business is able to monitor training completion and quality.	
PPCL3-AD-103	PPCL2-AD-013	**Assisted Digital**	The Supplier shall be prepared to partner with specialised training resources where the Supplier is unable to meet the specific training need so that staff are skilled appropriately	
PPCL3-AD-104	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide level of standards / accreditation required to meet training needs so that it is at an acceptable standard in line with government digital service management standards	
PPCL3-AD-105	PPCL2-AD-013	**Assisted Digital**	The Supplier shall ensure that when interacting with a Customer, the Agent has full access to the live retail website(s) and app(s) so that the Agent can view the same information at the same time as the Customer.	
PPCL3-AD-106	PPCL2-AD-013	**Assisted Digital**	The Supplier shall ensure that the agent has the necessary hardware, software and information so that the Agent is able to fully deal with Customer enquiries to ensure that the Customer maintains a seamless journey.	
PPCL3-AD-107	PPCL2-AD-013	**Assisted Digital**	The Supplier shall collaborate with other Suppliers to ensure that access to systems and data is available as required so that all staff have the tools required to perform their role.	
PPCL3-AD-108	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide test accounts for all systems so that the Director can effectively carry out assurance and oversight activities	
PPCL3-AD-109	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide appropriate tools and training (e.g. dummy accounts) to provide support for Digital champions so that agents are able to provide clarity and support Customers through a range of Customer journeys and other agents are supported as required	
PPCL3-AD-110	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide appropriate tools and training (e.g. dummy accounts) for Technical champions so that agents are able to provide clarity and support Customers through a range of Customer journeys and other agents are supported as required	
PPCL3-AD-111	PPCL2-AD-013	**Assisted Digital**	The Supplier shall offer British Sign Language where appropriate so that the communication needs of vulnerable Customers are supported.	
PPCL3-AD-112	PPCL2-AD-013	**Assisted Digital**	The Supplier will ensure agents respond to Customer interactions with the accurate information and in line with the Directors 'Tone of Voice' so that the response is factually correct, consistent and engaging.	
PPCL3-AD-113	PPCL2-AD-014	**Assisted Digital**	The Supplier shall provide the agent with the ability to see the Customers information and case progress through the stages of all contacts and processes so that the agent is able to view the progress and resolve the case to reduce the number of Customer interactions and improve Customer satisfaction	
PPCL3-AD-114	PPCL2-AD-014	**Assisted Digital**	The Supplier shall ensure that in-flight customer journeys are identified, monitored and managed, in-line with KPI's, so that interactions are resolved effectively and at first contact	
PPCL3-AD-115	PPCL2-AD-014	**Assisted Digital**	The Supplier shall ensure that the case management tools are integrated with all necessary systems (in collaboration with other Suppliers) so that the agents have access to all the information required to efficiently manage and complete the Customer journey and resolve the case	
PPCL3-AD-116	PPCL2-AD-014	**Assisted Digital**	The Supplier shall provide a case management system that retains all case information for a period aligned to the Directors retention schedule so that the business is able to review cases and operate assurance	
PPCL3-AD-117	PPCL2-AD-015	**Assisted Digital**	The Supplier shall ensure that the contact centre Agents access a consistent and accurate knowledge base with up to date information so that the Agents are able to help answer Customer enquiries.	
PPCL3-AD-118	PPCL2-AD-015	**Assisted Digital**	The Supplier in collaboration with the Director and other Suppliers shall ensure that FAQ information is up to date and relevant so that the Agent is able to quickly serve Customer queries	
PPCL3-AD-119	PPCL2-AD-016	**Assisted Digital**	The Supplier shall ensure that contact centre agents are able to support Customers with disabilities, restrictive mobility or other impairments so that Customers are serviced successfully and experience positive engaging interactions	

PPCL3-AD-120	PPCL2-AD-016	**Assisted Digital**	The Supplier shall be able to provide support services to Customers including, but not limited to; -Braille -Audio tape, Digital files or Physical -Large Print -Text relay service providing real-time service to support deaf, speech impaired and hearing -Call routing (to support vulnerable Customers in exceptional circumstances e.g. Covid) This is so that the business is able to support Customers with disabilities, restrictive mobility or other impairments and are serviced fully.	
PPCL3-AD-121	PPCL2-AD-016	**Assisted Digital**	The Supplier shall provide the ability to add and edit vulnerability markers to Customer accounts to indicate to the Agent when a Customer has a disability, vulnerability or is digitally excluded (with the ability to add and edit supporting commentary and context) so that the Agent is able to provide the correct level of service	
PPCL3-AD-122	PPCL2-AD-017	**Assisted Digital**	The Supplier shall conduct Customer satisfaction surveys, once approved by the Director, review and report on the survey results (including the ability to breakdown results by channel) so that the Director is able to review Customer feedback across all channels that this Supplier provides.	
PPCL3-AD-123	PPCL2-AD-017	**Assisted Digital**	The Supplier shall enable the capability for Agents to capture real-time Customer feedback so that the Supplier can improve the Customer experience	
PPCL3-AD-124	PPCL2-AD-017	**Assisted Digital**	The Supplier shall engage with the Director to regularly review and revise the survey content so that the surveys are aligned to brand principles and are relevant the Director's needs	
PPCL3-AD-125	PPCL2-AD-017	**Assisted Digital**	Supplier shall use Customer feedback (including but not limited to feedback received from or about other Suppliers) to compile a backlog of actions required so that the Supplier can improve the Customer experience	
PPCL3-AD-126	PPCL2-AD-017	**Assisted Digital**	The Supplier shall propose actionable insights addressing topics raised by Customer survey results so that the Director can consider options to improve the Customer experience	
PPCL3-AD-127	PPCL2-AD-017	**Assisted Digital**	The Supplier will collect and present Customer feedback surveys on an agreed frequency with the Director so that the business is able to adapt to Customer requirements as part of continuous improvement.	
PPCL3-AD-128	PPCL2-AD-017	**Assisted Digital**	The Supplier shall ensure that mechanisms are in place to understand why our Customers are contacting us including detailed Customer insight being made available so that the Business can see reasons for Customer contact and where problems are occurring in the main Customer journey's.	
PPCL3-AD-129	PPCL2-AD-017	**Assisted Digital**	The Supplier shall provide insights which gathers CSAT abandonment levels and Customer speed to complete so that the Supplier and Director can monitor CSAT performance	
PPCL3-AD-130	PPCL2-AD-017	**Assisted Digital**	The Supplier shall provide a facility to issue adhoc surveys to Customers via all channels and contact a selection of Customers so that feedback can be captured to help improve the service	
PPCL3-AD-131	PPCL2-AD-017	**Assisted Digital**	Supplier shall ensure that there is flexibility in the number of Customer surveys cap so that the business is able to adapt to requirements	
PPCL3-AD-132	PPCL2-AD-017	**Assisted Digital**	The Supplier shall provide access to the survey and reporting software so that the business is able to efficiently access the information and data.	
PPCL3-AD-133	PPCL2-AD-017	**Assisted Digital**	The Supplier shall provide specific ad hoc Customer insights ahead of required reporting frequencies so that live issues are raised in real-time allowing the Supplier and Director to implement rapid mitigating actions	
PPCL3-AD-134	PPCL2-AD-017	**Assisted Digital**	The Supplier shall ensure that vulnerable and digitally excluded Customers are able to access surveys so that we can capture data from all Customers.	
PPCL3-AD-135	PPCL2-AD-018	**Assisted Digital**	The Supplier shall collaboratively work with the Director and other Suppliers to map end to end Customer journeys so that the Director has oversight and can assure Customer journey experience	
PPCL3-AD-136	PPCL2-AD-018	**Assisted Digital**	The Supplier shall work with the Director and other Suppliers to develop seamless end-to-end digital services so that Customers are not deflected to offline channels by incompletely digitised processes or exceptions handling	
PPCL3-AD-137	PPCL2-AD-018	**Assisted Digital**	The Supplier in collaboration with the Director and other Suppliers shall apply a principle of 'accessibility by design' so that the Director is assured that deliverables are usable by Customers and agents across the spectrum of needs and abilities	
PPCL3-AD-138	PPCL2-AD-018	**Assisted Digital**	The Supplier shall collaborate with the Director and other Suppliers to design Customer journeys (in line with brand principles) and identify service improvement opportunities which are consistent across both self-service and Assisted Digital channels and touchpoints so that it is easy, engaging and seamless for the Customer.	
PPCL3-AD-139	PPCL2-AD-018	**Assisted Digital**	The Supplier in collaboration with the Director and other Suppliers shall ensure that a Customer can deflect their chat to an alternative channel that is available if required so that they can complete their jobs to be done.	
PPCL3-AD-140	PPCL2-AD-018	**Assisted Digital**	The Supplier in collaboration with the Director and other Suppliers shall ensure that the Agent is able to quickly access data and information as required to support Customers complete their jobs to be done so that the Customer receives an effective Customer journey.	
PPCL3-AD-141	PPCL2-AD-018	**Assisted Digital**	The Supplier in collaboration with the Director and other Suppliers shall ensure compliance with the Web Content Accessibility Guidelines WCAG 2.1 level AA (and any requirements later released), the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018, and the Equalities Act (2010) so that the Director is assured that the accessibility of its digital offer is compliant and that it treats Customers fairly	
PPCL3-AD-142	PPCL2-AD-018	**Assisted Digital**	The Supplier shall work with other Suppliers where required as part of accessibility testing, conducted by testers with representative vulnerabilities so that the Director is assured that services are usable by Customers across the spectrum of needs and abilities	
PPCL3-AD-143	PPCL2-AD-018	**Assisted Digital**	The Supplier shall collaborate with the Director and other Suppliers to review and agree the channel mix, including when to add or decommission channels so that the Director can maintain its fast follower status and meet Customer expectations	
PPCL3-AD-144	PPCL2-AD-011	**Assisted Digital**	The Supplier will ensure that the use of the Debit card facility complies with both the Director's security policy in this area and PCI DSS and provide regular assurance materials to demonstrate compliance as well as permit assurance activities as required by the Director	
PPCL3-AD-145	PPCL2-AD-011	**Assisted Digital**	The Supplier shall comply with PCI DSS and scheme rules for all Debit Card sales so that the Director remains compliant	
PPCL3-AD-146	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that Agents encourage Customers to deposit funds by the Director's preferred methods so that the business needs are met	
PPCL3-AD-147	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that contact centre Agents taking card payments confirm the Customer meets the criteria for making a deposit utilising systems provided by other Suppliers so that the Customer is able to complete their transactions and jobs to be done.	
PPCL3-AD-148	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that Agents are able to accept and enter repayment (money out) instructions from Customers (or nominated representatives), where it meets the security criteria in line with security policies, and only allow repayments if there are sufficient cleared funds available so that Customers can withdraw funds	
PPCL3-AD-149	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that Agents are able to accept and enter new or amended nominated account details (where it meets the security criteria in line with security policies) so that Customers (or nominated representatives) can withdraw funds	
PPCL3-AD-150	PPCL2-AD-011	**Assisted Digital**	The Supplier shall utilise all systems from other Suppliers to be able to make all payments in line with product terms and conditions so that Customer needs are met	
PPCL3-AD-151	PPCL2-AD-011	**Assisted Digital**	The Supplier shall work collaboratively with the Director and other Suppliers to reduce the number of debit card payments over time to more cost-effective payment channels so that the business runs efficiently	
PPCL3-AD-152	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that as new payment options come to market they are shared and reviewed with the Director in collaboration with other Suppliers prior to approval and implementation so that the business is able to seamlessly adapt to new processes with minimum Customer disruption	
PPCL3-AD-153	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that Agents are trained to use any new approved payment options so that the Agent is able to serve efficiently and the Customer has optimal payment options available	
PPCL3-AD-154	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that Agents are able to process in real-time internal product payment / transfers requests from Customers (e.g. premium bonds to direct saver) so that Customers can transfer between accounts	
PPCL3-AD-155	PPCL2-AD-011	**Assisted Digital**	The Supplier shall ensure that the Agent is able initiate payment of gifting requests in accordance with the Directors processes so that the Customer is able to make a gift to a minor.	
PPCL3-AD-156	PPCL2-AD-011	**Assisted Digital**	The Supplier shall provide Help content in a range of formats, including but not limited to: text, voice, visual, and video; so that a broad range of Customer needs are met.	
PPCL3-AD-157	PPCL2-AD-015	**Assisted Digital**	The Supplier shall optimise Help content, in collaboration with other Suppliers, so that searches (on both the Director's digital properties and external search engines) present relevant content to Customers.	
PPCL3-AD-158	PPCL2-AD-015	**Assisted Digital**	The Supplier shall tailor Help content to the different support touchpoints and Customer segments, so that the content directly engages a broad range of Customer audiences.	

PPCL3-AD-159	PPCL2-AD-015	**Assisted Digital**	The Supplier shall ensure that staff have the capability to provide content maintenance in the knowledge base that is easy to update and amend so that agents and Customers have up to an date and consistent knowledge base	
PPCL3-AD-160	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that the Customer is informed throughout the Customer journey relating to possible future interactions so that the Customer is well informed and does not need to contact the contact centre.	
PPCL3-AD-161	PPCL2-AD-001	**Assisted Digital**	The Supplier shall ensure that, in agreement with the Director, certain Customer facing services are provided with both English and Welsh language support so that the business remains compliant in line with the Welsh Language Act and Director's language scheme and Customers language needs are met.	
PPCL3-AD-162	PPCL2-AD-004	**Assisted Digital**	The Supplier shall collect and manage the Customers marketing preferences, operational communications and prize draw, and media preferences to be contacted/or receive notifications and through which channels so that Agents ensure that the Customer is able to determine what information is captured about them	
PPCL3-AD-163	PPCL2-AD-005	**Assisted Digital**	The Supplier will identify and review all automated responses on an agreed frequency with the Director so that reasons for contact are known so that frequent and emerging themes can be identified and new automated responses can be created.	
PPCL3-AD-164	PPCL2-AD-007	**Assisted Digital**	The Supplier shall provide a dedicated IFA phone line, and have the ability to commission new lines as required by the Director	
PPCL3-AD-165	PPCL2-AD-007	**Assisted Digital**	The Supplier shall enable the agents to identify the nature of the interaction, where it meets the security criteria and in line with security policies, before the Customer speaks so that the Agent can manage the Customer as effectively as possible	
PPCL3-AD-166	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that the Prize Draw results for all Premium Bond Customers are available via an automated capability so that both Prize Draw winners and losers can check the results	
PPCL3-AD-167	PPCL2-AD-007	**Assisted Digital**	The Supplier shall have the capability to provide Agent services for 366 days a year	
PPCL3-AD-168	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that the contact centre is available 24/7 for 366 days per year for the Virtual Agent/IVR so that Customers have optimal access to the contact centre	
PPCL3-AD-169	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that the financial advisor helpline email address is retained so that the service can maintain its current service	
PPCL3-AD-170	PPCL2-AD-009	**Assisted Digital**	The Supplier shall ensure that the Agent can identify the nature of the call for when connected to the Customer (e.g. recognising a recent event) so that the Agent has the required information speaking to a Customer.	
PPCL3-AD-171	PPCL2-AD-013	**Assisted Digital**	The Supplier shall provide access to test accounts for both Financial Advisors and Retail so that the business has visibility of the Financial Advisor portal	
PPCL3-AD-172	PPCL2-AD-013	**Assisted Digital**	The Supplier shall use agreed lines to take with the Director for all interactions with the Customer so that there is consistency in the messaging to the Customer	
PPCL3-AD-173	PPCL2-AD-015	**Assisted Digital**	The Supplier shall ensure that the contact centre Agents working on the financial advisor helpline access a consistent and accurate knowledge base with up to date information so that the Agents are able to help answer financial advisor enquiries	
PPCL3-AD-174	PPCL2-AD-018	**Assisted Digital**	The Supplier shall, in collaboration with the Director and other Suppliers, design and propose intuitive Assisted Digital experiences, so that future Operations staff find them easy to use.	
PPCL3-AD-175	PPCL2-OPS-001	**Assisted Digital**	The Supplier shall in collaboration with other Suppliers be able to take queries from Customers across all channels, investigate them in collaboration with other Suppliers (including trace of funds), and informs the Customer of the outcome so that the Customer has a seamless and effective Customer journey	
PPCL3-AD-176	PPCL2-AD-007	**Assisted Digital**	The Supplier shall ensure that if a Customer's information is not recognisable through the voice assistant/IVR prize checker capability, the Customer should be directed to a contact centre agent or to an appropriate digital channel so that the Customer is still able to check if they are a winner or not	
PPCL3-INT-001	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that the appropriate customer data can be amended by the customer or on behalf of the customer with appropriate control and authorisation, so that the Director and other Suppliers can ensure a complete record of its customers and population of the Digital Customer Profile.	
PPCL3-INT-002	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that the customer record is populated and updated with the customer vulnerability status where provided, so that the Director and its suppliers can provision the best service for its customers.	
PPCL3-INT-003	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that customers can provide new and updated data for inclusion into the customer record, so that the Director can ensure it has the most up to date information on all of its customers	
PPCL3-INT-004	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall deliver customer tailoring in a data-driven manner, so that the Director delivers the right services, at the right time, to the target customers	
PPCL3-INT-005	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that all tailoring within the service complies with legislation, guidelines and customers' expressed permissions, so that customers are treated fairly and in accordance with their rights	
PPCL3-INT-006	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall design, develop, and test customer tailoring as part of the Directors change mechanism, so that services are available for delivery to the appropriate customer needs	
PPCL3-INT-007	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure the tailoring of the service to customers responds to data updates, so that the relevant services are delivered to the customers	
PPCL3-INT-008	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall provide and make available to the Director and Other Suppliers data gathered from the provisioned and associated services, so that insights into service performance, customer impacts and customer behaviours can be developed	
PPCL3-INT-009	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall comply with agreed formats, delivery mechanisms, and schedules for all data provisions, so that the information remains consistent across the enterprise	
PPCL3-INT-010	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure the capability to receive and ingest Director provisioned data, so that the information remains consistent across the enterprise	
PPCL3-INT-011	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure the capability to receive and ingest data provisioned by other Suppliers, so that the information remains consistent across the enterprise	
PPCL3-INT-012	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall collaborate with other Suppliers and the Director on the sharing, ingestion and orchestration of data from source systems, so that a complete view of data is maintained across the enterprise	
PPCL3-INT-013	PPCL2-INT-002	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that all data captured from provisioned services and customer touchpoints can be joined to the Directors' customer records (including population of the Digital Customer Profile), so that the Director can maintain a complete view of all customer interactions and impacts into the service.	
PPCL3-INT-014	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight and recommendations on issues, opportunities, weaknesses and threats into the provisioned services, so that there are clear, actionable proposals for service developments and improvements to add to the backlog continuously	
PPCL3-INT-015	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight into the positive and negative impacts of proposed changes to the service, so that the business and customer benefits of changes are assessed and prioritised accordingly	
PPCL3-INT-016	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide data on the Supplier's operational performance, so that the Director can assure the service is appropriately managed	
PPCL3-INT-017	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall monitor the market and provide the Director with insight on customer experience enhancements, so that the Director can build a roadmap of change, prioritising improvements that assist the Directors in a position as fast follower in service provision and continues to meet customer expectations	
PPCL3-INT-018	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall contribute to the delivery of Service Delivery Measures (SDMs) and other success metrics (e.g. customer satisfaction) for the provisioned services, so that the Director is able to maintain continuity of business performance reporting (including to HM Treasury)	
PPCL3-INT-019	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall investigate fluctuations and trends in Service Delivery Measures (SDMs) and other success metrics, so that deviations in performance can be assessed and understood, driving continuous improvement to the Service	
PPCL3-INT-020	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide contextual analysis to all provisioned insights, so that the Director can interpret data and information in an appropriate manner according to how the service has been delivered	

PPCL3-INT-021	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Suppliers shall enable the Director to access all insights at any point in time, so that there is no disruption to the Directors operational agility	
PPCL3-INT-022	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide resource and capabilities for workforce and systems capacity forecasting, so that the Director and its Suppliers are able to optimise overall efficiency and productivity of the provisioned services	
PPCL3-INT-023	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide workforce and systems forecasting feedback and adjustment, so that the Director can ensure its resources are deployed in the most efficient way and to drive continuous improvement of the provisioned services	
PPCL3-INT-024	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall review and provide insight in response to change proposals from the Director, so that Good Industry Practice is considered and likely benefits or impacts can be measured, reviewed and taken into consideration before proceeding to development	
PPCL3-INT-025	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide Actionable Insight that states the case for changing the provisioned services, delivered to an agreed frequency and group of recipients, so that a prioritised backlog of continuous improvement and development of the provisioned services is enabled by robust and timely insight	
PPCL3-INT-026	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight into operational performance benchmarking for all of its provisioned services against the wider market, so that the Director can prioritise actions to improve the customer experience by closing gaps and taking opportunities	
PPCL3-INT-027	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide Actionable Insight to support prioritisation of change that will result in continuous improvement of the service and reduction in cost drivers, so that the Director can agree and drive improvements with other Suppliers based on the insight	
PPCL3-INT-028	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide Actionable Insights from the analysis of data collected across all customer touchpoints and channels including but not limited to, journey analytics, attitudinal research, and survey data so that there is a comprehensive view of the qualitative and quantitative performance of customer services available	
PPCL3-INT-029	PPCL2-INT-003	**Competitor, Service and Customer Intelligence**	The Supplier shall provide Actionable Insight into operational information, so that the drivers of interaction volumes, operational issues, and Supplier performance are understood by the Director	
PPCL3-INT-030	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight into all of their processes, so that the Director and its Suppliers can identify ways to improve the service through process improvement	
PPCL3-INT-031	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide information and insight when operational issues arise, so that the Director can avoid future service disruptions	
PPCL3-INT-032	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall agree with the Director on schedules and categories of operational reporting so that insights into the Supplier's operational effectiveness are easily accessed by the Director and Other Suppliers and drive effective business decisions	
PPCL3-INT-033	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide operational cost data, detailing transactional and other activity-based costs, which accurately describe the fixed and variable costs of the provisioned services, so that the Director can understand the drivers of cost at an event level	
PPCL3-INT-034	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide information on the methodology used to calculate activity-based-cost drivers at the most granular level and how these quantify the supplier's operational processes, so that the Director can deliver a roadmap of cost-effective change.	
PPCL3-INT-035	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall append activity-based-costs to the customer record that captures customer interactions, so that the Director and it Suppliers can understand the drivers of customer value and make recommendations on future operational improvements	
PPCL3-INT-036	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight into it service performance (e.g. process times, wait times, back logs etc), so that the Director and its Suppliers can keep its customers informed of its services.	
PPCL3-INT-037	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide the capability to deliver insight on workload capacity levels, so that the Director is able to forecast workforce demand and make the service more efficient or leverage all opportunities where capacity is available	
PPCL3-INT-038	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide access to all data types (including structured, semi-structured and rich data attributes) to the Director and its Suppliers, so that the Director has the ability to ingest all data into its eco-system and leverage that data for improved and tailored services to customers	
PPCL3-INT-039	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide actionable insight for the Supplier provisioned services, so that the Director can be assured that the Supplier is continuously improving it's service	
PPCL3-INT-040	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall provide ongoing insights into the performance of newly implemented improvements so that the impact of any new service can be assessed and further continuous improvement is actioned	
PPCL3-INT-041	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure capture and availability of resource and workload data, so that the Director is assured of operational delivery	
PPCL3-INT-042	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall track and provide insight on all customer journeys including channel deflections (e.g. from digital self-service channels to Assisted Digital channels and vice versa), so that the Director can improve its service and ensure all customer needs are met	
PPCL3-INT-043	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall collaborate with the Director to propose journey, experience and message changes, so that the Director can continuously improve its customer experience and create a prioritised plan to remove pain points	
PPCL3-INT-044	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall capture and provide insights about its Non-Digital and Assisted Digital customer journeys (e.g. call interactions, Social Media, Chat Bot interactions), so that the Director and its Suppliers can understand and action necessary service improvements	
PPCL3-INT-045	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight and service usage patterns aligned to the Director's customer and market segmentation, customer personas (including vulnerable / digitally excluded customer personas) and Jobs to be Done framework, so that the Director and its Suppliers can understand who and how the service is being used and build a roadmap to improve services targeted to customer needs.	
PPCL3-INT-046	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight on customer and service user sentiments, so that the Director and its Suppliers can understand and action necessary service improvements	
PPCL3-INT-047	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight on time in process for all provisioned customer journeys, so that the Director can understand and its Suppliers understand and action required service improvements and tailor its content to drive better understanding of response times	
PPCL3-INT-048	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall provide insight on customer interactions which require additional resource for resolution, so that the Director and its Suppliers can understand and action necessary service improvements	
PPCL3-INT-049	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall analyse and evaluate any changes that have been implemented to their provisioned services, so that the Director can accurately assess whether recommendations are driving incremental improvements to the service.	
PPCL3-INT-050	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall comply with the Director's audit processes and complete identified actions, so that the Director can assure quality in the provisioned services, data governance standards are adhered to and the provisioned services continuously improve.	
PPCL3-INT-051	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall control access to provisioned insights, so that authorised users are able to view and perform actions on data and insights relevant to their role.	
PPCL3-INT-052	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall comply with the Directors data standards so that the provisioned data and information is trusted by the Director and its suppliers.	
PPCL3-INT-053	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that any insights tools or provisioned insight are appropriate for use and storage within the Directors organisation and are in line with the agreed security & compliance requirements, so that customer data is protected and the Director reduces legal and regulatory risk in line with the outlined risk appetite	

PPCL3-INT-054	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that all insights are available in the Director's centralised library, so that the Directors users and its suppliers have a single location to easily access all of its supplier insights	
PPCL3-INT-055	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure compliance with the Director's Customer Data Retention Rules (CDRR), so that the Director's data is retained for an appropriate length of time which reduces exposure to negative financial and reputational impact	
PPCL3-INT-056	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure compliance with the Director's Information Asset Management handbook, so that the Director has a complete view of all of its assets which reduces exposure to negative financial and reputational impact	
PPCL3-INT-057	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall engage with, support and complete actions arising from the Director's data governance committees, working groups and processes, so that the Director can assure the Supplier is effectively managing its data and is performing its responsibilities as a data steward	
PPCL3-INT-058	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure a timely rectification of any identified data issues (including the systems, people and processes that create, update and manage the Director's data), so that data governance standards are adhered to and the Director reduces its exposure to negative financial and reputational impact	
PPCL3-INT-059	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall capture and maintain data about the Supplier provisioned resources and services in line with the Director's Data Capture standards, so that the Director can assure the appropriate availability of data and insight to make business decisions	
PPCL3-INT-060	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall regularly review and agree changes to customer permissions, attributes, and data under its management, so that there is an agreed, and joint roadmap for improving, adding and combining data sources, which enables the Director to improve and tailor its customer service	
PPCL3-INT-061	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall ingest and act upon changes in customer permissions, attributes, and data provided by the Director and its suppliers, so that new data sources are leveraged to support decision making and improvements to the customer experience	
PPCL3-INT-062	PPCL2-INT-001	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure customers who need to contact the Director via the Supplier's Provisioned Services can have their customer data populated and updated with correct authorisation (e.g. but not limited to the Death Claims Process, exMinor claims process), so that the customer can manage the account directly without restriction through digital channels	
PPCL3-INT-063	PPCL2-INT-004	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure access to the Director and Other Suppliers to all metadata about its provisioned services, so that the Director and Other Suppliers have a complete record relating to the Supplier provisioned services	
PPCL3-INT-064	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that all of its provisioned services are informed and operationally ready for the Directors prescribed engagement with its customers through below-the-line and above-the-line marketing, so that operational fallout from these campaigns is communicated and handled by the Supplier through an easy and pre-agreed process	
PPCL3-INT-065	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that its provisioned services can be tailored to customers according to actionable insights, so that the Director can assure the best service for its customers when they interact through the customer touchpoints.	
PPCL3-INT-066	PPCL2-INT-005	**Competitor, Service and Customer Intelligence**	The Supplier shall ensure that its provisioned services can be tailored to customers with a vulnerability status, so that the Director can assure the best service for its customers when they interact through the customer touchpoints.	
PPCL3-INT-067	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall agree and adhere to a metadata framework across all provisioned services, so that the Director and other Suppliers can understand how data has been collected, its timeliness, and the corresponding data descriptions	
PPCL3-INT-068	PPCL2-INT-006	**Competitor, Service and Customer Intelligence**	The Supplier shall provide information on all the available data and metadata (including, but not limited to, data models, business glossaries and data dictionaries) to the Director and other Suppliers, so that the Director can understand and leverage all of its data across the Enterprise	
PPCL3-CM-01	PPCL2-CMP-001	**Complaints Management**	The Supplier will retain historic complaint data as agreed, including that migrated from previous supplier, so that the supplier and the Director have access to all relevant complaint history.	
PPCL3-CM-02	PPCL2-CMP-001	**Complaints Management**	The Supplier will register all complaints on to an integrated complaints system so that they are accessible to all authorised staff and the Director.	
PPCL3-CM-03	PPCL2-CMP-001	**Complaints Management**	The Supplier shall operate a complaints management process that covers all service Channels through which Customers can contact the Director to highlight a level of dissatisfaction, so that all complaints are accurately captured.	
PPCL3-CM-04	PPCL2-CMP-001	**Complaints Management**	The Supplier shall aim to resolve and close a minimum set target of complaints within 3 days after receipt. The Supplier shall also contact the customer via phone (using call recorded system) to proactively resolve complaints within 3 days after receipt so that customers are dealt with instantly and customers are left satisfied.	
PPCL3-CM-05	PPCL2-CMP-001	**Complaints Management**	The Supplier will acknowledge receipt of correspondence to the complainant in line with the Directors complaint handling policy so that the customer is aware that the complaint is being processed.	
PPCL3-CM-06	PPCL2-CMP-001	**Complaints Management**	The Supplier shall record all incoming and outgoing complaint correspondence onto the integrated complaint system which is accessible to specific agreed Director teams so that assurance and oversight can be given.	
PPCL3-CM-07	PPCL2-CMP-001	**Complaints Management**	The Supplier shall provide fully trained teams to identify, register and resolve all complaints so that all complaints are appropriately dealt with.	
PPCL3-CM-08	PPCL2-CMP-001	**Complaints Management**	The Supplier shall provide appropriate responses to customers which address all of their complaint points, so that customers are appropriately and fairly dealt with.	
PPCL3-CM-09	PPCL2-CMP-001	**Complaints Management**	Where necessary the Supplier will seek clarification from the complainant to resolve any issue raised, so that an appropriate outcome is determined and a positive customer experience is ensured.	
PPCL3-CM-10	PPCL2-CMP-001	**Complaints Management**	The Supplier shall provide customer satisfaction feedback ensuring that it reaches a minimum standard that is agreed with the Director so that customer experience is ensured.	
PPCL3-CM-11	PPCL2-CMP-001	**Complaints Management**	The Supplier will deal with all outstanding complaints, so that all complaints are resolved in accordance with the Director's complaints Handling Policy.	
PPCL3-CM-12	PPCL2-CMP-001	**Complaints Management**	During Complaint handling, the Supplier shall identify and record where necessary customer vulnerability. They will action reasonable adjustments when handling complaints for vulnerable customers in line with the Vulnerable Customers Policy so that customer experience is positive.	
PPCL3-CM-13	PPCL2-CMP-001	**Complaints Management**	The Supplier shall identify adaptive requirements based on accessibility so that all customers needs are in line with Equality Act.	
PPCL3-CM-14	PPCL2-CMP-001	**Complaints Management**	Once the customer has completed authentication, the Supplier's Complaint Service Representative will then cross check customer details at point of service, so that customers are not mis-identified and ensuring that the complaint system does not have different customer details to other systems.	
PPCL3-CM-15	PPCL2-CMP-002	**Complaints Management**	The Supplier will operate processes and controls to ensure all complaints are correctly identified and captured for processing when they are first raised regardless of channel, medium or team receiving the complaint, so that all complaints are dealt with in an appropriate and timely manner	
PPCL3-CM-16	PPCL2-CMP-002	**Complaints Management**	The Supplier will identify and register all Complaints in accordance with relevant regulation and the Director's Complaints Handling Policy so that complaints can be dealt with appropriately	
PPCL3-CM-17	PPCL2-CMP-002	**Complaints Management**	The Supplier will uniquely identify the customer complaint/correspondence to enable identification of any engagements, aligned to that customers so that all related correspondence is linked and can be easily accessed and reviewed together.	
PPCL3-CM-18	PPCL2-CMP-002	**Complaints Management**	The Supplier shall collate and record engagement via multiple channels the same complaint, so that complaints are not duplicated and all related correspondence/engagement records can be reviewed together.	
PPCL3-CM-19	PPCL2-CMP-002	**Complaints Management**	The Supplier will have the capability to efficiently search and access for all individual customer engagement records relating to the same complaint, so that all related customer correspondence is easily accessible allowing efficient customer servicing/complaint resolution.	
PPCL3-CM-20	PPCL2-CMP-002	**Complaints Management**	The Supplier will log the channel through which the complaint is raised (e.g. phone, internet, post, email) to record how the complaint is being registered by the customer, so that It is clear for Complaint Service Representatives how the complaint was raised and they can note this in their correspondence to customers	
PPCL3-CM-21	PPCL2-CMP-002	**Complaints Management**	The Supplier shall identify and record the "type" of complaint to categorise appropriately including Other Suppliers, so that complaints are efficiently directed to the appropriate functions/personnel for resolution.	
PPCL3-CM-22	PPCL2-CMP-002	**Complaints Management**	Should any complaint not be identified at first point of contact, the Supplier will ensure, that when they are identified, they are recorded as backdated and actioned accordingly, so that no complaints are left unhandled and appropriate urgency can be applied to those identified "late".	

PPCL3-CM-23	PPCL2-CMP-002	**Complaints Management**	The Supplier will ensure all relevant staff are trained appropriately regarding complaint handling, and that evidence of successful training is retained with assurance statements. The Director shall be provided with monthly MI on training completed for assurance purposes, allowing for the ability to raise/challenge or query.	
PPCL3-CM-24	PPCL2-CMP-002	**Complaints Management**	The Supplier shall supply the Director with monthly MI and assurance statements regarding the training status of all personnel who may receive/process complaints, so that the Director can be assured of the Training and Competence of the relevant staff.	
PPCL3-CM-25	PPCL2-CMP-003	**Complaints Management**	The Supplier will operate an agreed escalation process/framework. This will identify various scenarios that require appropriate and co-ordinated handling of specific complaint escalations in line with the Director's policy.	
PPCL3-CM-26	PPCL2-CMP-003	**Complaints Management**	The Supplier will define and operate processes for when receiving and handling a complaint from a vulnerable customer, to ensure the appropriate identification of vulnerability, treatment, escalation and resolution in accordance with the Director's policy and regulation so that complaints being raised by vulnerable customers are actioned appropriately.	
PPCL3-CM-27	PPCL2-CMP-003	**Complaints Management**	The Supplier will agree with the Director and then operate a process to identify specific defined key indicators of customer financial hardship and escalate/ resolve accordingly so that the complaints of those customers so affected are appropriately handled and resolved.	
PPCL3-CM-28	PPCL2-CMP-003	**Complaints Management**	The Supplier will define and operate a process and escalations to manage a complaint where the customer mentions the Freedom of Information Act (FOI). This will include a customer acknowledgement and confirmation of the FOI request and will be dealt with within the complaint response, so that the customers request is appropriately dealt with and the matter is notified to the Director at the correct time.	
PPCL3-CM-29	PPCL2-CMP-003	**Complaints Management**	The Supplier shall ensure any complaints related to fraud will be passed on to the relevant team and other supplier, so that the escalation follows the appropriate channels.	
PPCL3-CM-30	PPCL2-CMP-003	**Complaints Management**	The Supplier will identify and appropriately action complaints regarding urgent payments. This will include the "immediate" handling and resolution of the matter within the 3 working day period, so that the Director is meeting the requirements in resolving complaints promptly	
PPCL3-CM-31	PPCL2-CMP-003	**Complaints Management**	The Supplier will ensure that all Complaint Service Representatives recognise and escalate any cases which indicate fraudulent activities, so that the appropriate personnel / teams are notified and can operate required processes. This will include the Financial Crime team.	
PPCL3-CM-32	PPCL2-CMP-003	**Complaints Management**	The Supplier will ensure that all Complaint Service Representatives recognise and escalate all cases which indicate media involvement (or potential media involvement) so that the correct staff / management deal with media related enquires and appropriate escalations/involvement of the Director is made.	
PPCL3-CM-33	PPCL2-CMP-003	**Complaints Management**	The Supplier will provide a service that requires the closure of reported issues to be "owned" by the Complaint Service Representative, so that issues relating to complaints are monitored and driven to completion by the Complaints team.(This will involve collaboration between suppliers)	
PPCL3-CM-34	PPCL2-CMP-004	**Complaints Management**	The Supplier will require the Complaint Service Representative to be able to review any complaint related requested actions as well as view up to date status on any correspondence/actions so that the Complaint Service Representative can effectively drive the accurate and timely completion of the matter.	
PPCL3-CM-35	PPCL2-CMP-004	**Complaints Management**	The Supplier will have effective tools in place to allow the Complaint Service Representatives to deal with cases themselves so that, they can effectively and individually manage cases to resolution.	
PPCL3-CM-36	PPCL2-CMP-004	**Complaints Management**	The Supplier shall operate a process where complaints that are unable to be resolved by the Complaint Service Representative , are then escalated to the correct area of the business including Other Suppliers so they can be dealt with accurately and fairly in a timely manner.	
PPCL3-CM-37	PPCL2-CMP-005	**Complaints Management**	The Supplier shall have the ability to forward specialist complaints received via the HMT channel to senior management (of the Directors) to respond appropriately within agreed timeframes so that the supplier adheres to terms of reference and Directors memo to HMT.	
PPCL3-CM-38	PPCL2-CMP-005	**Complaints Management**	The Supplier will obtain appropriate sign off from the Director prior to responses being to sent to customers regarding Specialist complaints so that the Director can provide specific oversight to these particular complaints.	
PPCL3-CM-39	PPCL2-CMP-005	**Complaints Management**	The Supplier will adhere to the terms of reference in relation to HMT and the Director so that quality responses are provided in a timely manner.	
PPCL3-CM-40	PPCL2-CMP-005	**Complaints Management**	The Supplier shall provide the Director with accurate information to update the media with so that brand and reputational damage is mitigated	
PPCL3-CM-41	PPCL2-CMP-006	**Complaints Management**	The Supplier will operate a system whereby if a customer updates their 'Details' whilst a complaint is live, then this will be automatically reflected across the complaint record so that the complaint customer records are kept up to date. 'Details' could include but are not limited to (extensive): Name, address, telephone numbers, markers of vulnerability, accessibility requirements, account closures, payment requests, change of bank details, providing Evidence of Identity, legal authority, requesting statements, personal details, update security	
PPCL3-CM-42	PPCL2-CMP-006	**Complaints Management**	When handling complaints, the Supplier shall update customer information accurately across the business, including within solutions provided by Other Suppliers', so that customer information can be consistently maintained across all platforms.	
PPCL3-CM-43	PPCL2-CMP-007	**Complaints Management**	The Supplier will ensure that their Complaint Service Representative have the ability to view all customer information, their business correspondence and complaint record across all platforms and systems and channels so that the Complaint Service Representative can deal with complaint investigations efficiently.	
PPCL3-CM-44	PPCL2-CMP-007	**Complaints Management**	The Supplier shall provide the Director with the ability and permissions to view all customer correspondence and information across all supplier systems so that the Director can have undertake effective oversight and assurance regarding complaint management	
PPCL3-CM-46	PPCL2-CMP-008	**Complaints Management**	The Supplier will identify and categorise any large incident/policy complaint and if a specific complaint type exceeds a threshold then an incident must be raised and escalated to the Director so that these complaints can be dealt with consistently and appropriately.	
PPCL3-CM-47	PPCL2-CMP-008	**Complaints Management**	The Supplier will operate a process whereby if an incident/large issue occurs a notification of the incident is issued to the appropriate teams/ complaint department including the agreed lines to take, so that the Complaint Service Representative can update customers consistently.	
PPCL3-CM-48	PPCL2-CMP-008	**Complaints Management**	The Supplier will develop incident related complaint responses with the Director so that large incident related complaints are appropriately and consistently dealt with in line with the Director's agreement	
PPCL3-CM-49	PPCL2-CMP-008	**Complaints Management**	The Supplier shall propose and agree with The Director, tailored incident complaint responses for vulnerable customers if required, so that all groups are fairly dealt with in line with Directors agreement.	
PPCL3-CM-50	PPCL2-CMP-008	**Complaints Management**	The Supplier will ensure that agreed responses are updated inline with lessons learned and feedback provided to the areas where improvement is needed, so that if further insight is gained from feedback/ lessons learned our responses can be further tailored to address this.	
PPCL3-CM-51	PPCL2-CMP-008	**Complaints Management**	The Supplier shall create and maintain a compensation matrix for the Director's approval. This will then be used to ensure that consistent compensation payments that are made to customers as appropriate without case by case reference to the Director. The Supplier will obtain the Director's approval of the matrix annually and at any point where change becomes required.	
PPCL3-CM-52	PPCL2-CMP-009	**Complaints Management**	The Supplier will ensure that all compensation payments made to customers are in line with the agreed matrix so that compensation amounts are consistently paid to customers who experience similar compensatable issues	

PPCL3-CM-53	PPCL2-CMP-009	**Complaints Management**	The Supplier will provide and maintain relevant training to address compensation scenarios so that complaints requiring compensation are resolved fairly.	
PPCL3-CM-54	PPCL2-CMP-009	**Complaints Management**	The Supplier will maintain a record of the rationale used when deciding which compensation case/award has been used in each individual case of compensation.	
PPCL3-CM-55	PPCL2-CMP-009	**Complaints Management**	The Supplier will maintain a record of all compensation agreed/paid and will report this to the Director on a monthly basis for review.	
PPCL3-CM-56	PPCL2-CMP-010	**Complaints Management**	The Supplier shall record the appropriate root cause against each complaint in a timely manner to assist analysis, insight and recommendations so that processes and customer satisfaction are improved.	
PPCL3-CM-57	PPCL2-CMP-010	**Complaints Management**	The Supplier shall operate a controlled process and system to hold, add and update root cause types/categories so that root cause types available to be allocated to complaints can be adjusted over time to ensure they remain relevant.	
PPCL3-CM-58	PPCL2-CMP-010	**Complaints Management**	The Supplier shall operate a controlled process and system to hold, add and update "sub-sets" of root cause types/categories so that root cause type "sub-sets" are available to be allocated to complaints can be adjusted over time to ensure they remain relevant.	
PPCL3-CM-59	PPCL2-CMP-010	**Complaints Management**	The Supplier shall ensure the Complaint Service Representatives have the ability to raise emerging issues/ themes for review so that it can be escalated to the correct teams at the relevant Supplier.	
PPCL3-CM-60	PPCL2-CMP-010	**Complaints Management**	The Supplier will provide the capability for the Director to have relevant permissioned access to review the MI, the root cause analyse records and monitoring tools so that the Director can operate assurance and oversight.	
PPCL3-CM-61	PPCL2-CMP-010	**Complaints Management**	The Supplier shall provide evidence to support Complaints MI regarding Complaints logged and closed on request , so that the Director can operate effective oversight of complaints handling.	
PPCL3-CM-62	PPCL2-CMP-010	**Complaints Management**	The Supplier shall be proactive in regularly making and actioning recommendations to address findings from the root cause analysis so that there is continuous improvement for customer experience and complaint volumes associated with the root cause reduce/are eradicated.	
PPCL3-CM-63	PPCL2-CMP-010	**Complaints Management**	The Supplier will operate a process to allow The Director to engage in feedback/discussion regarding MI/Root causes and actions proposed by the Supplier, so that the Director can challenge / propose action plans and dialogue with the Supplier to improve customer outcomes.	
PPCL3-CM-64	PPCL2-CMP-011	**Complaints Management**	The Supplier shall produce Complaints MI reporting so that the Director can assure the complaint reporting before publishing results in line with FCA requirements.	
PPCL3-CM-65	PPCL2-CMP-011	**Complaints Management**	The Supplier shall produce Complaints MI reporting every six months and when requested. Reporting shall include but no the limited to total complaints, received, closed, upheld and be produced in line with FCA requirements, so that the Director can have oversight and assurance, and accurate and timely reporting of complaints can be made to the regulator.	
PPCL3-CM-66	PPCL2-CMP-011	**Complaints Management**	The Supplier shall operate a process to receive and act upon/respond to the Director's feedback on complaints data and reporting provided (produced and submitted), so that the Director can challenge and assure the information.	
PPCL3-CM-67	PPCL2-CMP-012	**Complaints Management**	The Supplier will handle all operations and processes regarding the registration with FOS of complaints and will respond where necessary to the Financial Ombudsman Service (FOS) in relation to FOS referred customer complaint, so that The Director's involvement is limited to oversight and assurance.	
PPCL3-CM-68	PPCL2-CMP-012	**Complaints Management**	The Supplier shall provide The Director with at a minimum monthly reporting on FOS volumes and cases in line with FOS reporting standards. This will include; cases received, cases closed, assessments issued and ombudsman final decisions. The Supplier will also provide such reporting to The Director on an adhoc/on request basis, so that the Director receives assurances the cases are being dealt with a timely manner.	
PPCL3-CM-69	PPCL2-CMP-012	**Complaints Management**	The Supplier shall reimburse to the Director for all invoices monthly for FOS service (upheld cases to be paid for by supplier) as well as paying for the annual levy so that the Director is not required to pay for the costs of FOS cases or service	
PPCL3-CM-70	PPCL2-CMP-012	**Complaints Management**	The Supplier will adhere to requests from FOS in line within the agreed timelines both operationally and in line with any vulnerability and accessibility needs identified by FOS, so that these cases will be dealt with in an appropriate and timely manner	
PPCL3-CM-71	PPCL2-CMP-012	**Complaints Management**	The Supplier shall ensure all actions arising from reporting discussions with FOS are carried out and evidenced so that all tasks are actioned in an accurate and timely manner and assurance can be demonstrated of their completion.	
PPCL3-CM-72	PPCL2-CMP-012	**Complaints Management**	The Supplier shall ensure that lessons learned and feedback reviews will be held with the Director if similar complaints are escalated to FOS which they uphold, so that action can be taken to improve process/services and reduce the specific type of complaint with confirmation being provided to The Director when this has been completed.	
PPCL3-CM-73	PPCL2-CMP-012	**Complaints Management**	The Supplier will provide the Director with a monthly report of all FOS cases including closures, new cases, all open cases and all relevant information pertaining to these. The report will also be provided when the Director requests it on an adhoc basis.	
PPCL3-CM-74	PPCL2-CMP-013	**Complaints Management**	The Supplier shall operate the agreed mechanism to use the data collated to identify and provide feedback to Other Suppliers where causes of complaints are attributed to that supplier, so that areas of weakness are identified and Other Suppliers commit to actions being taken to improve and actions are tracked to completion.	
PPCL3-CM-75	PPCL2-CMP-013	**Complaints Management**	Having identified the occurrence of a root cause the Supplier will monitor any further complaints attributed to that cause, so that reoccurrences are tracked and minimised.	
PPCL3-CM-76	PPCL2-CMP-013	**Complaints Management**	The Supplier shall demonstrate and evidence effective change having been implemented in response to root cause analysis, including that taken by Other Suppliers. This will form part of the regular reporting so that a reduction in the recurrence of the complaint root cause can be witnessed by the Director.	
PPCL3-CM-77	PPCL2-CMP-014	**Complaints Management**	The Supplier shall identify whether a complaint is related to any Data Protection issues, so that it can be escalated to the appropriate areas of the business to ensure correct handling in line with specific requirements.	
PPCL3-CM-78	PPCL2-CMP-014	**Complaints Management**	The Supplier shall ensure complaints relating to Data Protection breaches are managed/handled in line with the relevant data protection legislation so that the Director remain compliant.	
PPCL3-RC-013	PPCL2-RC-004	**Compliance**	The supplier shall comply with all legal and regulatory equivalence, that NS&I are subject to or that a fully regulated deposit-taker in the market would be subject to, at all times, including when there are changes or newly added regulations and legislation in line with regulatory developments, so that the Director and the Services remain compliant	The Supplier shall comply with all legislations set out in the Director's Compliance Universe document, which is subject to change, in-line with regulatory developments.
PPCL3-RC-014	PPCL2-RC-004	**Compliance**	The Supplier shall provide a solution that ensures that all data subjects' rights requests are fulfilled, in collaboration with Other Suppliers, so that the Director can respond to the request within regulatory timescales.	
PPCL3-RC-015	PPCL2-RC-004	**Compliance**	The Supplier shall collaborate with the Director in a timely manner when a request for information is made under the Freedom of Information Act so that the Director can respond to the request within regulatory timescales.	
PPCL3-RC-016	PPCL2-RC-004	**Compliance**	The Supplier shall ensure that affected customers are provided with relevant compliance notifications (including, but not limited to, changes to T&Cs and interest rate notifications) within agreed timescales, so that the Director complies with their regulatory obligations related to the information to be provided to customers.	
PPCL3-RC-017	PPCL2-RC-005	**Compliance**	The Supplier shall provide assurance that relevant personnel are trained and operating in compliance with financial service industry standards.	
PPCL3-RC-018	PPCL2-RC-005	**Compliance**	The Supplier shall enable the Director, should they wish, to assure any compliance training plans and/or materials, so that the Director is confident that the supplied team is operating within financial service industry standards.	
PPCL3-RC-019	PPCL2-RC-005	**Compliance**	The Supplier shall provide suitably experienced staff, with Compliance and legal knowledge, so that the operations run compliantly in-line with compliance and data protection requirements	

PPCL3-RC-020	PPCL2-RC-005	**Compliance**	The Supplier shall provide suitably experienced staff that are able to respond to comprehensively and appropriately to data subject rights requests, so that the Director complies with their obligations under UK GDPR	
PPCL3-RC-021	PPCL2-RC-005	**Compliance**	The Supplier shall ensure that its staff are adequately trained to identify Freedom of Information requests and forward them to the Director in a timely manner so that the Director can respond to the request with regulatory timescales	
PPCL3-RC-022	PPCL2-RC-006	**Compliance**	The Supplier shall store data in the UK.	
PPCL3-RC-023	PPCL2-RC-006	**Compliance**	The Supplier shall ensure all 3rd parties contracted also adhere to UK data hosting and storage requirements.	
PPCL3-RC-024	PPCL2-RC-006	**Compliance**	The Supplier shall ensure that any data stored throughout the duration of contract, is done so in line with the Directors retention schedule so that the Director is compliant with the necessary legal requirements and standards.	
PPCL3-DM-01	PPCL2-DPM-001	**Document Management**	The Supplier shall ensure secure storage so that all customer related documents can be held and retrieved in line with the Directors requirements and policies.	
PPCL3-DM-02	PPCL2-DPM-001	**Document Management**	The Supplier shall ensure physical and electronic storage provided can meet demand, so that the customer related documents are all appropriately held.	
PPCL3-DM-03	PPCL2-DPM-001	**Document Management**	The Supplier to provide physical access to appropriate sites upon request so that the Director can have oversight and carry out assurance activities on physical documents and systems that manage them.	
PPCL3-DM-05	PPCL2-DPM-001	**Document Management**	The Supplier shall be able to store and retrieve customer related documents from all relevant systems and storage, so that the Directors services are not interrupted.	
PPCL3-DM-06	PPCL2-DPM-001	**Document Management**	The Supplier shall have the capability to receive and return physical documents via different mail options, including but not limited to, standard mail, recorded mail, special, foreign, so that customer requests can be met.	
PPCL3-DM-07	PPCL2-DPM-001	**Document Management**	The Supplier shall provide the capability to share digitised documentation with Other Suppliers, so that a complete view of customer communications is maintained across the enterprise.	
PPCL3-DM-08	PPCL2-DPM-001	**Document Management**	The Supplier shall provide capability to receive and return customer documents so that necessary internal processes can be fulfilled.	
PPCL3-DM-09	PPCL2-DPM-001	**Document Management**	The Supplier shall ensure an efficient retrieval process for physical customer documents is provided, so that requests for documents can be fulfilled in a timely manner as agreed with the Director.	
PPCL3-DM-10	PPCL2-DPM-001	**Document Management**	The Supplier to have a process in place whereby when physical documents are retrieved from storage they should be digitised and stored in a legally admissible format and the physical copy destroyed inline with agreed the Directors RIM Data Destruction Disposal Policy' so that the physical document is no longer required. **Assumption of legally admissible format**	
PPCL3-DM-11	PPCL2-DPM-001	**Document Management**	The Supplier shall have a process in place to destroy documents in line with the customer document retention repository CDRR schedule so that the Director can comply with the relevant legislation.	
PPCL3-DM-12	PPCL2-DPM-001	**Document Management**	The Supplier shall ensure that compliance/regulatory standards are met and all relevant information and data is available as requested so that the Director can adhere to the relevant policies.	
PPCL3-DM-13	PPCL2-DPM-001	**Document Management**	The Supplier shall monitor the market and provide the Director with insight on alternative methods of physical documentation storage and digitisation , so that the Director retains its fast follower status and drives an efficient service.	
PPCL3-DM-14	PPCL2-DPM-001	**Document Management**	The Supplier shall provide recommendations on how to manage storage/retrieval historic physical and microfiche documents, so that these documents are accounted for.	
PPCL3-DM-15	PPCL2-DPM-001	**Document Management**	The Supplier shall provide the Director access to a shared repository with Other Suppliers for documentation such as not limited to SOPS, journey maps, quality framework and reconciliation process, so that the Director can have oversight and assurance.	
PPCL3-DM-16	PPCL2-DPM-002	**Document Management**	The Supplier shall ensure that all inbound physical documents are digitised, exploring options such as but not limited to, scanning and optical character recognition tools so that digitised version of the document, and its meta data, can be stored and processed by the Directors and Other Suppliers systems.	
PPCL3-DM-17	PPCL2-DPM-002	**Document Management**	The Supplier shall agree with the Director and implement the agreed recommendation on how to manage historic, physical and microfiche documents so that the documents are secure and available.	
PPCL3-DM-18	PPCL2-DPM-002	**Document Management**	The Supplier shall ensure inbound physical customer correspondence are scanned, so that processes can be completed in accordance with agreed KPIs.	
PPCL3-DM-19	PPCL2-DPM-003	**Document Management**	The Supplier shall provide the capabilities to search for documents by a range of key terms and meta data, so that the Director and its suppliers can locate information in order to provision services.	
PPCL3-DM-20	PPCL2-DPM-003	**Document Management**	The Supplier shall provide relevant resource, expertise and people to review and change document contents, so that the Directors content remains compliant, accurate and relevant.	
PPCL3-DM-21	PPCL2-DPM-003	**Document Management**	The Supplier shall ensure that provisions are in place to support delivery of physical paper documents, so that the Director can communicate with its customers through their chosen channel.	
PPCL3-DM-22	PPCL2-DPM-003	**Document Management**	The Supplier shall collaborate with the other Director suppliers to facilitate the delivery of digital documents, so that the Director can communicate with its customer through their chosen channel.	
PPCL3-DM-23	PPCL2-DPM-004	**Document Management**	The Supplier shall be able to receive and open the mail at a secure facility at all level of requirements (e.g. regardless of postal classification) in line with KPI so that all customer requirements can be met.	
PPCL3-DM-24	PPCL2-DPM-004	**Document Management**	The Supplier shall ensure that all mail is received for processing and collected for dispatch in line with agreed KPIs, so that the customer experiences an efficient service.	
PPCL3-DM-25	PPCL2-DPM-004	**Document Management**	The Supplier shall be able to securely store any incoming mail not processed on the day of arrival, so that it can be processed on the next business day.	
PPCL3-DM-26	PPCL2-DPM-004	**Document Management**	The Supplier shall receive and return different types of legal documents, (including but not limited to passports, wills, death certificates) by the appropriate postal classification including but not limited to, standard mail, recorded mail, special, foreign, within agreed KPI, so that customer documents are returned in line with Directors guidelines.	
PPCL3-DM-27	PPCL2-DPM-004	**Document Management**	The Supplier to have the capability to apply modern print fulfilment and mailing standards (e.g. print on demand, selective insertion, sustainability) so that the Director can run an efficient and cost effective outbound postal capability.	
PPCL3-DM-28	PPCL2-DPM-004	**Document Management**	The Supplier shall ensure that all mail is received for processing and collected for dispatch in line with agreed SLAs, so that the customer experiences an efficient service.	
PPCL3-DM-29	PPCL2-DPM-004	**Document Management**	The Supplier shall have documented processes in place for dealing with inbound post and outbound print in agreement with the Director so that the Director has appropriate oversight and assurance	
PPCL3-DM-31	PPCL2-DPM-004	**Document Management**	The Supplier shall be able to make changes/amendments to outbound paper and electronic customer related documents if required and agreed with the Director, and in line with the agreed timeline so that the documents are up to date.	
PPCL3-DM-32	PPCL2-DPM-005	**Document Management**	The Supplier shall be able to identify all incoming mail and prioritise this in agreement with the Director and inline with the Directors timelines so that customer documentation is routed to the appropriate workflow for processing.	
PPCL3-DM-33	PPCL2-DPM-005	**Document Management**	The Supplier shall provide and operate a Case Management System for items coming in via post and are scanned into the correct workflow, so that incoming items can be reconciled and are accurately accounted for, and processed in a timely manner.	
PPCL3-DM-34	PPCL2-DPM-005	**Document Management**	The Supplier to have the capability to use technology to efficiently sort, digitise categorise and gather meta data about inbound paper documents so that the Director can benefit from effective and efficient process.	
PPCL3-DM-35	PPCL2-DPM-005	**Document Management**	The Supplier shall provide a search and retrieval mechanism that enables Other Suppliers to be able to search for, and retrieve, the digitised documents along with the related meta-data so that they can be used as required by that supplier	
PPCL3-DM-36	PPCL2-DPM-005	**Document Management**	The Supplier shall allow the Director to carry out all agreed assurance and oversight actions related to the processing of documents	
PPCL3-DM-37	PPCL2-DPM-005	**Document Management**	The Supplier shall ensure they have the capability and compatibility to scan paper documents to the appropriate area within the workflow system so that operational processing can be completed.	
PPCL3-DM-38	PPCL2-DPM-005	**Document Management**	The Supplier shall provide adaptable dashboards which shows details (e.g. headcount, holdovers etc) that help show the service performance and which help to prevent any resource gaps or any issues so that the business is able to run an effective and seamless service for the Customer.	
PPCL3-DM-39	PPCL2-DPM-006	**Document Management**	The Supplier will utilise agreed templates and data including from Other Suppliers to create all customer documents, including electronic and physical format, so that all customer correspondence is of a consistent standard.	
PPCL3-DM-40	PPCL2-DPM-006	**Document Management**	The Supplier shall work collaboratively with all Other Suppliers, to get relevant information to ensure correspondence to customers is accurate and dealt in a timely manner.	

PPCL3-DM-42	PPCL2-DPM-006	**Document Management**	The Supplier shall provide and maintain an electronic repository of outbound customer related documents, including but not limited to letters, forms, templates, brochures, T&Cs, statements, maturity letters, so that the Director can have a full and accurate record of customer related documents.	
PPCL3-DM-43	PPCL2-DPM-006	**Document Management**	The Supplier shall work collaboratively with the Director, its partners and chosen external agencies to create new or amend outbound customer communications when required, so that policy and business objectives are met and/or line to changes to products and/or services.	
PPCL3-DM-44	PPCL2-DPM-006	**Document Management**	The Supplier shall collaborate (with the Director and chosen agencies) in the design of customer marketing communications as agreed by the Director, so that the Director can assure the quality of outputs and leverage supplier and agency domain expertise.	
PPCL3-DM-45	PPCL2-DPM-006	**Document Management**	The Supplier shall produce customer marketing communications as agreed with the Director, so that the correct information is provided to the customer effectively and efficiently.	
PPCL3-DM-46	PPCL2-DPM-006	**Document Management**	The Supplier shall utilise industry standard software and hardware for the creation and production of customer marketing communications, so that collaborative working can be facilitated.	
PPCL3-DM-47	PPCL2-DPM-006	**Document Management**	The Supplier shall apply Director brand guidelines, content and communications strategy and other standards (including accessibility regulations, and inclusive design), so that all customer communication outputs are consistent, designed for all users, reach desired levels of quality and customer experience and support business objectives.	
PPCL3-DM-48	PPCL2-DPM-006	**Document Management**	The Supplier shall provide content design and production capabilities to produce high quality paper and electronic communications and make sure that training and support is in place for those producing the content to continually refresh their skills and understanding of best practice.	
PPCL3-DM-49	PPCL2-DPM-006	**Document Management**	The Supplier shall provide a system that enables tagging of all outbound mandatory customer communications, so that the supplier and Director can recall items for different scenarios. (e.g. retrieving all correspondence relating to a specific stage of a customer journey)	
PPCL3-DM-50	PPCL2-DPM-006	**Document Management**	The Supplier shall provide a system that can ingest and work industry standard file types (including but not limited to InDesign, Adobe Creative Suite, HTML), so that outputs created by Other Suppliers can be taken into the system without the need to recreate them in the document management system.	
PPCL3-DM-51	PPCL2-DPM-006	**Document Management**	The Supplier shall use behavioural science knowledge and insight in the design of specifics templates and forms so that the customer and the Director benefit and to improve end to end process success.	
PPCL3-DM-52	PPCL2-DPM-006	**Document Management**	The Supplier shall ensure that the Director has sight of supplier training plans and at request the ability to input to training material so that the business remains compliant and staff operate to a high standard.	
PPCL3-DM-53	PPCL2-DPM-006	**Document Management**	The Supplier will need to be able to make changes to outbound paper and electronic customer related templates if required and agreed with the Director, and in line within the agreed timeline so that the documents are up to date.	
PPCL3-DM-54	PPCL2-DPM-007	**Document Management**	The Supplier shall ensure there is a process in place to identify any correspondence received in Welsh in line with agreed procedures, so that the business remains compliant and customers language needs are met. .	
PPCL3-DM-55	PPCL2-DPM-007	**Document Management**	The Supplier shall work with Other Suppliers to get relevant information so that the correct data is used to create and produce relevant correspondence across the enterprise in relation to the data sharing agreement.	
PPCL3-DM-56	PPCL2-DPM-007	**Document Management**	The Supplier shall ensure that document management services are made available to Other Suppliers in an efficient and secure manner so that customers can be serviced in line with the Directors requirements"	
PPCL3-DM-57	PPCL2-DPM-007	**Document Management**	The Supplier shall ensure that all document related customer interactions are correctly recorded against the customers digital profile so that the Director can obtain a complete view of all customer interactions"	
PPCL3-DM-58	PPCL2-DPM-008	**Document Management**	The Supplier shall have the ability to print on demand so that the storage of pre-printed documents is not required.	
PPCL3-DM-59	PPCL2-DPM-008	**Document Management**	The Supplier shall provide a scalable print capacity that is able to deliver, including but not limited, large batch printing, small batch printing and individual documents in a timely manner so that the Director can provide an efficient service for its customers.	
PPCL3-DM-60	PPCL2-DPM-008	**Document Management**	The Supplier shall provide the Director with management information (MI) related to its printing services so that the Director can measure their success against their digital/non digital targets.	
PPCL3-DM-61	PPCL2-DPM-008	**Document Management**	The Supplier shall provide cost effective and environmentally friendly printing solutions in agreement with the Director so that the Director can meet its sustainability and cost reduction targets.	
PPCL3-DM-62	PPCL2-DPM-008	**Document Management**	The Supplier shall provide printed proofs for The Director as part of workflow to approve when required by the Director so that quality of printed outputs reaches required brand standards, and that all customers have the required levels of customer experience.	
PPCL3-DM-63	PPCL2-DPM-008	**Document Management**	The Supplier shall print outbound customer communications to timelines agreed with the Director and have the flexibility to deliver according to the Directors business critical timescales, so that we can deliver policy and regulatory directives quickly.	
PPCL3-DM-64	PPCL2-DPM-008	**Document Management**	The Supplier shall manage and order stock suppliers, including but not limited to, envelopes and paper, so that demand can be met and the Directors services are not interrupted.	
PPCL3-DM-65	PPCL2-DPM-009	**Document Management**	The Supplier shall be able to compose, print, control and dispatch warrants in line with the Directors requirements so that non-digital payments are available for those customers that need them	
PPCL3-DM-66	PPCL2-DPM-009	**Document Management**	The Supplier to ensure warrants and warrant stationery are held securely so that the Directors security requirements are met.	
PPCL3-DM-67	PPCL2-DPM-009	**Document Management**	The Supplier shall be able to order and manage its stock of warrant stationery in line with demand so that wastage is prevented	
PPCL3-DM-68	PPCL2-DPM-009	**Document Management**	The Supplier shall be able to make any required changes to the warrant templates and that appropriate testing is in place to meet industry standards, so that Directors requirements can be met.	
PPCL3-DM-69	PPCL2-DPM-009	**Document Management**	The Supplier shall ensure there is an appropriate reconciliation process that can be evidenced, so that there is a complete and accurate record of including but not limited to production, dispatch, file transfer, work volumes and relevant systems.	
PPCL3-DM-70	PPCL2-DPM-009	**Document Management**	The Supplier shall ensure that warrants issued meet all regulatory requirements, so that the Director remains compliant.	
PPCL3-DM-71	PPCL2-DPM-009	**Document Management**	The Supplier shall work collaboratively on warrant stationery design with Director and appropriate suppliers so that warrants meet both regulatory and brand requirements	
PPCL3-DM-72	PPCL2-DPM-010	**Document Management**	The Supplier shall provide a system that enables the creation, storage, management, version control, composition and visualisation of document templates and documents from a single interface so that the Director can efficiently manage their templates and documents."	
PPCL3-DM-73	PPCL2-DPM-010	**Document Management**	The Supplier to ensure the appropriate resourcing is in place to create, amend and change document templates within agreed timelines, so that Director is assured outputs are correct and up to date.	
PPCL3-DM-74	PPCL2-DPM-010	**Document Management**	The Supplier shall provide capability to search/design/deliver/tag static content that are deployed across multiple templates so that the Director can deliver changes as efficiently as possible. (e.g. when telephone number changes to change not just individual asset but across all)	
PPCL3-DM-75	PPCL2-DPM-010	**Document Management**	The Supplier shall ensure that all changes to a template are auditable and version controlled so that the correct version of a template can be used to compose a document	
PPCL3-DM-76	PPCL2-DPM-010	**Document Management**	The Supplier shall provide the Director suitable access to the template management solution so that template review and approval actions can be carried out.	
PPCL3-DM-77	PPCL2-DPM-010	**Document Management**	The Supplier shall provide a collaborative review and approval system for document templates under its control so that the Director can approve and retain ownership of document templates.	
PPCL3-DM-78	PPCL2-DPM-010	**Document Management**	The Supplier shall subject all templates to comprehensive testing so that quality can be assured	
PPCL3-DM-79	PPCL2-DPM-011	**Document Management**	The Supplier to ensure there is an auditable change control testing/governance in place for electronic and printed documents including but not limited to physical checking quality of documents so that assurance and oversight can take place.	

PPCL3-DM-80	PPCL2-DPM-011	**Document Management**	The Supplier shall have the flexibility to adhere to the Directors requests on an adhoc basis of newly specified electronic and printed documents including but not limited to letters, forms, lines to take so that the Directors requirements are met.	
PPCL3-DM-81	PPCL2-DPM-011	**Document Management**	The Supplier shall have the capability complete, capture and evidence end to end (e2e) testing of any changes to new electronic /paper outputs and prints so that oversight and assurance can take place.	
PPCL3-DM-82	PPCL2-DPM-011	**Document Management**	The Supplier shall collaborate with the Director and its chosen agencies to provide a robust and flexible processes for ongoing review of all customer related documents and templates and to have final approval of amendments made by the supplier to outputs so that customer communications can be produced according to brand and compliance standards.	
PPCL3-DM-83	PPCL2-DPM-011	**Document Management**	The Supplier to be aware of new technology and information to improve the efficiency of testing (and to implement if in agreement with the Director)so that the Director is a fast follower of innovation inline with industry best practices.	
PPCL3-DM-84	PPCL2-DPM-011	**Document Management**	The Supplier will collaborate with Other Suppliers to be able to receive and process cheques in a secure and timely manner, so that these are progressed through to the bank clearing house.	
PPCL3-DM-85	PPCL2-DPM-012	**Document Management**	The Supplier will collaborate with Other Suppliers to be able to receive and process cheques, so that customer funds are credited to the account in a secure and timely manner.	
PPCL3-DM-86	PPCL2-DPM-012	**Document Management**	The Supplier shall have a process that can deal with the return of unacceptable cheques and applications that do not meet the Directors T&Cs in a timely manner, so that customers are aware and can take the appropriate next steps.	
PPCL3-DM-87	PPCL2-DPM-012	**Document Management**	The Supplier shall monitor the market and provide the Director with insight on alternative methods of processing and imaging cheques , so that the Director retains its fast follower status and drives an efficient service.	
PPCL3-DM-88	PPCL2-DPM-012	**Document Management**	The Supplier shall scan cheques and store the cheque and image for the agreed amount of time in line with the Directors agreement, so that the Director meets the requirements for handling cheques.	
PPCL3-DM-89	PPCL2-DPM-012	**Document Management**	The Supplier shall securely hold, and then deposit, any post-dated customer cheques received for a period set by the Director, so that the customers sale can be processed at the appropriate time.	
PPCL3-DM-90	PPCL2-DPM-012	**Document Management**	The Supplier shall track and return any cash received, so that customers find an alternative way to pay in line with Directors T&Cs and has assurance that payment has been returned.	
PPCL3-DM-91	PPCL2-DPM-012	**Document Management**	The Supplier shall have an effective/automated reconciliation process in agreement with the Director so that the Directors banking activities are appropriately operated and controlled.	
PPCL3-DM-92	PPCL2-DPM-013	**Document Management**	The Supplier shall ensure that it has the capability to apply structured data about its customer related documents so that the Director and its suppliers understand the full set of documents under its control.	
PPCL3-DM-93	PPCL2-DPM-013	**Document Management**	The Supplier shall ensure that it has the capability to apply semi structured data about the contents of each customer related document, including but not limited to tagging content parts, so that the Director can understand elements of our communications that are applied across multiple documents.	
PPCL3-DM-94	PPCL2-DPM-013	**Document Management**	The Supplier shall ensure that it has the capability to apply and store sufficient meta data about its customer related documents, so that the Director has a complete view of the lifecycle of the document and the document can be utilised for the delivery of relevant customer services.	
PPCL3-DM-95	PPCL2-DPM-014	**Document Management**	The Supplier shall enable the Director and its suppliers to work with the correct versions of documents held within the supplier system so that customers, the Director and its suppliers can have the correct documents available to them through their preferred channels.	
PPCL3-DM-96	PPCL2-DPM-014	**Document Management**	The Supplier shall have a system in place to present customers with the version of document they have been served in their engagement with Director, so that the customer, the Director and its suppliers has a complete view of all the interactions with the Director.	
PPCL3-FC-001	PPCL2-FC-001	**Financial Crime**	The Supplier shall appoint a Money Laundering Reporting Officer (MLRO) and a Nominated Officer (Optional for one person to carry out both roles). The MLRO will have responsibility for raising all Suspicious Activity Reports (SAR's) to the National Crime Agency (Within agreed timeframes with the Director) so that the the Supplier does not put the Director in breach of money laundering and related reporting compliance under relevant UK legislations (Proceeds of Crime Act, Money Laundering and Terrorism Act).	
PPCL3-FC-002	PPCL2-FC-001	**Financial Crime**	The Supplier shall assess and review the configuration of the financial crime screening and consult with "Other Suppliers" to apply changes so that the screening is continuously governed and improved upon when possible	
PPCL3-FC-003	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure all customers are appropriately investigated against Politically Exposed Persons (PEP) lists and have appropriate measures in place to deal with true matches to both high and low risk PEP's so that the Director can comply with the Money Laundering Regulations by ensuring controls are in place to monitor and assess higher risk customers under PEP status.	
PPCL3-FC-004	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure there is a process in place to monitor PEPs transactional activity, changes to customer account and also any adverse media related to a True PEP match, so that the Director can comply with enhanced due diligence obligations under the Money Laundering Regulations.	
PPCL3-FC-005	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure there is appropriate processes in place to screen for sanctioned individuals both at on boarding stages and throughout a customer lifecycle using various trigger points to highlight any requirement to re-screen (Sanctions list being updated/change of customer name/payment in or out) so that the Director can ensure compliance with financial sanctions.	
PPCL3-FC-006	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure there is appropriate internal escalation routes within the suppliers Financial Crime Team when dealing with PEP and sanctions matches including higher risk scenarios related to adverse media and suspicious activity report (SAR's) so that appropriate governance and oversight is in place to deal with higher risk scenario's.	
PPCL3-FC-007	PPCL2-FC-001	**Financial Crime**	The Supplier shall make appropriate use of a false positive "white list" increasing efficiency and false positive rates throughout the duration of screening customers when possible so the number of false positive alerts can be reduced	
PPCL3-FC-008	PPCL2-FC-001	**Financial Crime**	The Supplier shall have a case management system in place to organise, handle and review all cases dealt with by the Financial Crime team across Fraud, PEP's, Money Laundering and Terrorist Financing alerts and Sanctions Alerts. This should have the facility to upload evidence in cases for audit and also have capability for analysts to leave notes on cases, available to view by any analyst should it re-alert in the future so that the financial crime team have access to all financial crime case data assets in a single source location which is easily accessible for data retention, audit and assurance purposes	
PPCL3-FC-009	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure there is processes in place to handle reporting to and handling enquiries including court orders from external agencies when required to do so in relation to Office of Financial Sanctions Implementation (OFSI), National Crime Agency (NCA), Action Fraud and Serious Fraud Office so the Director can ensure compliance with financial crime legislations applying to the Director.	
PPCL3-FC-010	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure the appointed MLRO is responsible for compliance with the FCA's rules on systems and controls against money laundering so the Director and Supplier can comply with the FCA's rules on systems and controls against money laundering.	
PPCL3-FC-011	PPCL2-FC-001	**Financial Crime**	The Supplier shall ensure the financial crime function is designed and operates in line with guidance from the UK's Joint Money Laundering Steering Group and the FCA Financial Crime Guide: A firm's guide to countering financial crime risks. The Supplier shall ensure any future revisions of such guidance are adhered to and applied to the Directors outsourced Financial Crime Function so that the Director and supplier are aligned in the systems and control environment of the outsourced financial crime work	
PPCL3-FC-012	PPCL2-FC-002	**Financial Crime**	The Supplier shall comply with the Directors Customer Due Diligence Policy and align all processes and controls for Customer Due Diligence with this, so that the Director can comply with the Customer Due Diligence obligations under the UK Money Laundering Regulations	
PPCL3-FC-013	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure there are controls in place to prevent customers who fail to pass customer due diligence checks from carrying out a transaction. When a sale is attempted and the customer fails Customer Due Diligence checks in line with the Directors Customer Due Diligence Policy, the funds should be refunded to the source bank account used for the deposit so that the Director can remain compliant with the UK Money Laundering Regulations (Requirement to cease transactions)	
PPCL3-FC-014	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure there is processes in place to highlight instances of fraudulent methods to set up fraudulent accounts via fake documentation or stolen identities so the Director can ensure financial crime customer due diligence mitigations are in place for fraudulent account set up	

PPCL3-FC-015	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure there are processes and controls in place to escalate suspicions regarding Customer Due Diligence information obtained, and take action to report this to the National Crime Agency if necessary so that the Director can comply with the suspicion reporting requirements under Money Laundering, Terrorist Financing and Transfer of funds (Information on the Payee) Regulations 2017 Act.	
PPCL3-FC-016	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure there are trigger points in place to update and review Customer Due Diligence in line with Joint Money Laundering Steering Group guidance so that the Supplier and Director complies with ongoing monitoring for the purposes of the UK Money Laundering Regulations customer due diligence requirements.	
PPCL3-FC-017	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure a risk based process is maintained to request further information regarding Customer Due Diligence, including where necessary, enhanced due diligence so the Director and Supplier can comply with requirements of ongoing monitoring under the UK Money Laundering Regulations.	
PPCL3-FC-018	PPCL2-FC-002	**Financial Crime**	The Supplier should have processes in place to obtain source of wealth and source of funds, both at customer on-boarding stages and for the purposes of on-going monitoring so that the Director and the Supplier can comply with the ongoing monitoring requirements under the UK Money Laundering Regulations.	
PPCL3-FC-019	PPCL2-FC-002	**Financial Crime**	The Supplier shall ensure Customer Due Diligence processes for on boarding are designed to utilise a Trusted Electronic Evidence of Identity provider, relying on evidence of identity documentation when required to do so that the service is aligned to guidance from the Joint Money Laundering Steering Group	
PPCL3-FC-020	PPCL2-FC-003	**Financial Crime**	The Supplier shall ensure the contact centre are trained to spot the signs of fraud on a Customer account and liaise with the Suppliers Financial Crime team to help mitigate fraud as soon as possible so that there is a clear process in place between the call centre, the Suppliers Financial Crime team and Other Suppliers to ensure suspicions reported via the call centre are acted upon and investigated	
PPCL3-FC-021	PPCL2-FC-003	**Financial Crime**	The contact centre shall have the ability to leave notes on a customer account in relation to suspicious activity being reported by Customers to the Director. This should then be escalated to the Suppliers Relevant Financial Crime SME to apply safeguards to a customer account so that there is a clear audit trail of events in relation to financial crime being reported on a customer account	
PPCL3-FC-022	PPCL2-FC-003	**Financial Crime**	The Supplier shall ensure they maintain customer communication on how to prevent fraud on their accounts and provide information on this via all applicable channels (phone/online/contact centre) to ensure knowledge is shared with the Directors customers on keeping their savings safe	
PPCL3-FC-023	PPCL2-FC-003	**Financial Crime**	The Supplier should ensure there is an easy and accessible route for customers to raise concerns/suspicions to the Director in relation to their account across all applicable channels each NS&I product offer so that the Directors customers can safely raise concerns about the accounts they operate.	
PPCL3-FC-026	PPCL2-FC-003	**Financial Crime**	The Supplier shall have processes in place to ensure vulnerable customers can conduct business with the Director and have Financial Crime processes in place to deal with any heightened risk which may come with a vulnerable customer so that the Directors business remains inclusive to all types of customers and there are safeguards in place to mitigate financial crime in light of risks presented to vulnerable customers'.	
PPCL3-FC-027	PPCL2-FC-004	**Financial Crime**	The Supplier shall have a case management system in place to deal with all applicable elements of financial crime work, which is digital and shows a clear audit trail of events in any case dealt with so that all relevant financial crime information is retained appropriately and is easily accessible for the purposes of investigations, audit and assurance	
PPCL3-FC-028	PPCL2-FC-004	**Financial Crime**	The Supplier shall ensure the case management system used has the facility to upload documentation to it in relation to each case handled. The system should have the facility to add notes from analysts and also be easy to locate cases historically for a set period of time agreed with the Director so that the outcome and rationale for each case is documented and retained for the purposes of investigation, audit and assurance purposes.	
PPCL3-FC-029	PPCL2-FC-004	**Financial Crime**	The System should have the ability to easily display previous cases worked with the rationales previously used available to the analysts working the cases so that there is a continuation of alert history and clear trail of events in dealing with each case	
PPCL3-FC-030	PPCL2-FC-004	**Financial Crime**	The Supplier shall ensure there are read only licences available for the Director's staff to use on the case management system both for the Director's audit and assurance purposes so that the Director can remain informed on the performance of financial crime work	
PPCL3-FC-031	PPCL2-FC-004	**Financial Crime**	The Supplier will provide accessibility to completed cases across financial crime work to the Directors staff for the purposes of assurance so that the Director remains informed on the performance of financial crime work	
PPCL3-FC-032	PPCL2-FC-004	**Financial Crime**	The Supplier shall train staff on their responsibilities within their roles towards financial crime compliance. The Supplier shall provide the Director with oversight of training materials used for the Suppliers financial crime team. All appointed individuals working on Financial Crime work should be suitably skilled and have knowledge on what their roles require of them, this should either be pre-employment or provided during the training period of employment. Ongoing training should also be provided to all staff on their Financial Crime responsibilities so that suitably skilled staff are in place for financial crime work and remain suitably skilled within their financial crime roles	
PPCL3-FC-033	PPCL2-FC-005	**Financial Crime**	The Supplier shall ensure there is a reporting pack which is shared with the Director on a monthly basis covering all financial crime Key Risk Indicators & Key Risk Controls. The reporting pack should consist of Management Information (MI) which clearly details the performance of Financial Crime across all applicable elements of financial crime work so that the Director remains informed on the performance of the financial crime function	
PPCL3-FC-034	PPCL2-FC-005	**Financial Crime**	The Supplier shall continue to assess the effectiveness at mitigating financial crime and report on the effectiveness of the financial crime alerts on a monthly basis so that the performance of the Suppliers financial crime team can continuously improve and the Director remains informed on the performance of the financial crime function	
PPCL3-FC-035	PPCL2-FC-005	**Financial Crime**	The Supplier shall carry out regular horizon scanning to ensure compliance with all applicable Financial Crime laws applying to the Director so the Director can be compliant with changes to laws applying to the Directors business	
PPCL3-FC-036	PPCL2-FC-005	**Financial Crime**	The Supplier shall carry out annual Money Laundering & Terrorist Financing Risk Assessment on behalf of the Director so that the Director can be well informed on the performance of the financial crime function	
PPCL3-FC-037	PPCL2-FC-005	**Financial Crime**	The Supplier shall maintain their own Anti-Bribery and Corruption Policy and aligned to the Directors Bribery & Corruption Policy so that safeguards are in place to ensure the Director is compliant with the Bribery Act including any agency/outsourcer carrying out work on behalf of the Director and Supplier.	
PPCL3-FC-038	PPCL2-FC-005	**Financial Crime**	The Supplier shall carry out a Bribery and Corruption Risk Assessment in relation to the Directors work annually so the Director can be informed on the risk environment in which the supplier operates with regards to Bribery & Corruption	
PPCL3-FC-039	PPCL2-FC-005	**Financial Crime**	The Supplier shall carry out an annual fraud risk assessment detailing the performance of anti-fraud measures to ensure improvement upon existing measures when possible so the Director can be informed on the fraud risks and performance of fraud mitigations related to the Director's business.	
PPCL3-FC-040	PPCL2-FC-005	**Financial Crime**	The Supplier shall ensure the Suppliers senior management approval is required for all policies, processes and controls applied to mitigate financial crime so that appropriate governance is in place involving management	
PPCL3-FC-043	PPCL2-FC-005	**Financial Crime**	The Supplier shall analyse customer and transactional trends to assess the effectiveness so that the supplier may adapt financial crime rules based on sound analysis of financial crime risks	
PPCL3-FC-045	PPCL2-FC-006	**Financial Crime**	The Supplier shall have controls in place to actively highlight instances of Money Laundering, Terrorist Financing, Fraud and Tax Evasion and have internal escalation routes to raise this with the NCA so that the Director can comply with reporting obligations under various UK Financial Crime legislations	
PPCL3-FC-046	PPCL2-FC-006	**Financial Crime**	The Supplier shall maintain controls to mitigate fraud being carried out both internally and externally so that the funds under the Directors management remain secure and have safeguards to mitigate and prevent fraud	
PPCL3-FC-047	ut	**Financial Crime**	The Supplier shall have processes in place to screen the Directors customers for politically exposed persons and screen against all applicable Sanctions lists (OFSI, UN, OFAC, EU) so that the Director can comply with UK sanctions and Money Laundering legislations	
PPCL3-FC-048	PPCL2-FC-006	**Financial Crime**	The Supplier shall ensure the Suppliers business rules to mitigate financial crime are regularly reviewed each quarter and the outcome of the reviews are shared with the Director so that the Director can be confident risks to the business are reviewed regularly for financial crime	
PPCL3-FC-049	PPCL2-FC-006	**Financial Crime**	The Supplier shall ensure all data sets made available by the Director are utilised and considered in the creation of the Suppliers financial crime business rules, so that there is a range of information that can be utilised for the purposes of a risk based approach to mitigating financial crime	
PPCL3-FC-050	PPCL2-FC-006	**Financial Crime**	The Supplier shall facilitate a Financial Crime monthly governance meeting between the Director, the supplier and 'Other Suppliers', so that key financial crime matters can be discussed between all suppliers and the Director.	
PPCL3-FC-051	PPCL2-FC-006	**Financial Crime**	The Supplier shall operate 3 lines of defence governance model so that appropriate oversight and assurance of the business is in place.	

PPCL3-FC-052	PPCL2-FC-007	**Financial Crime**	The Supplier shall take into account multiple risk factors when authenticating customers and apply additional security when required (for instance when a customer has a change of device being used for logging in, IP Address change, address change, name change, change of nominated bank details) so that the Directors funds under management can be secure from fraudulent access attempts	
PPCL3-FC-053	PPCL2-FC-007	**Financial Crime**	The Supplier shall apply a risk-based approach towards applying Strong Customer Authentication and ensuring compliance with the Regulatory Technical Standard of the Payment Services Regulations 2017, so that the Director's funds under management can be secure from fraudulent access attempts	The Supplier shall apply a risk based approach towards utilising Strong Customer Authentication and ensuring compliance with Regulatory Technical Standards as defined in the payments service regulations so that the Director's funds under management can be secure from fraudulent access attempts
PPCL3-FC-054	PPCL2-FC-007	**Financial Crime**	The Supplier shall implement a process/control to block access when a customer has too many attempts to log into their account so that fraudulent access attempts can be limited and mitigated	
PPCL3-FC-055	PPCL2-FC-007	**Financial Crime**	The Supplier shall have processes in place to securely re-set customer log in details securely, and through channels offered under each product so that all customers have the ability to manage re-setting forgotten details to access their products	
PPCL3-FC-056	PPCL2-FC-007	**Financial Crime**	The Supplier shall set risk tolerances for all capabilities in accordance with the Directors policies and risk tolerance so that there is a uniform approach to risk management across all areas	
PPCL3-FC-057	PPCL2-FC-008	**Financial Crime**	The Supplier shall ensure there is processes in place to log staff access to Customer accounts and the Supplier shall be able to use this information during any investigation of internal fraud so that any internal investigation can be based on analysis of the systems used for Customer interactions	
PPCL3-FC-058	PPCL2-FC-008	**Financial Crime**	The Supplier shall ensure a risk assessment is carried out against staff access on the banking engine ensuring each staff only have access to what is required within their individual roles so there is appropriate segregation of access tailored to what access a staff member requires to avoid internal errors and minimise opportunity for fraud and data theft.	
PPCL3-FC-065	PPCL2-FC-010	**Financial Crime**	The Supplier shall ensure the ability to forecast alert volumes across financial crime work and ensure there is sufficient staffing in place to work all financial crime alerts within appropriate timescales agreed with the Director so that the financial crime operations operates efficiently and workloads are kept under control, minimizing customer impact	
PPCL3-FC-066	PPCL2-FC-010	**Financial Crime (Business Continuity)**	Supplier shall ensure the systems utilised for mitigating financial crime are resilient and have been tested against industry recognised business continuity standards so there is limited impact on the financial crime operations in the event of incidents	
PPCL3-FC-067	PPCL2-FC-010	**Financial Crime**	The Supplier shall ensure the Director is notified of any incident in relation to the financial crime systems, controls, processes or policies within agreed timescales so that the Director is kept informed on risks to the financial crime operations.	
PPCL3-FC-068	PPCL2-FC-010	**Financial Crime**	The Supplier shall ensure any rules and controls configurations made for the purposes of financial crime is agreed with the Director via Financial Crime governance forums. Changes made to the systems rules and controls should also take into account any staffing levels so that the Director has appropriate oversight of changes made to the financial crime controls, systems rules and processes	
PPCL3-FC-069	PPCL2-FC-010	**Financial Crime**	The Supplier shall share information with the Director related to the amount of staff involved for financial crime work and also information related to financial crime alert volumes across all financial crime work so the Director has appropriate oversight of financial crime operations	
PPCL3-FC-070	PPCL2-FC-011	**Financial Crime**	The Supplier shall have policies, processes and controls to manage and mitigate financial crime threats. This will be governed by a monthly forum with the Directors Financial Crime team to ensure alignment on the approach to mitigate the risk of Financial Crime	
PPCL3-FC-071	PPCL2-FC-011	**Financial Crime**	The Supplier shall set the controls and configurations of all financial crime processes, controls and systems and ensure this is shared with the Director so that the Director is well informed on the performance of the financial crime function	
PPCL3-OPS-01	PPCL2-OPS-001	**Non-Digital Operational Processing**	The Supplier shall ensure that all supportive sub-processes (in relation to, but not limited to bereavement, sales, payments etc) are completed effectively and efficiently so that Customer jobs to be done are completed	
PPCL3-OPS-02	PPCL2-OPS-002	**Non-Digital Operational Processing**	The Supplier shall ensure that Customers with sensitive queries, including but not limited to bereavement, power of attorney, are dealt with by appropriately trained staff so that Customers receive an appropriate service in difficult circumstances.	
PPCL3-OPS-03	PPCL2-OPS-002	**Non-Digital Operational Processing**	The Supplier shall process bereavement claims in line in with agreed priorities set by the Director, so that any urgent claims are dealt efficiently including but not limited to, funeral expenses.	
PPCL3-OPS-04	PPCL2-OPS-002	**Non-Digital Operational Processing**	The Supplier shall ensure that all relevant Customer records are checked in line with standard procedures so that estate claims are settled completely.	
PPCL3-OPS-05	PPCL2-OPS-002	**Non-Digital Operational Processing**	The Supplier shall complete robust checks to ensure the appropriate legal representative is identified so that the claim is settled correctly in line with the legal representative instructions.	
PPCL3-OPS-06	PPCL2-OPS-002	**Non-Digital Operational Processing**	The Supplier shall explore alternative approaches that specialist services (e.g. 'Tell me once')/family/legal representatives could use to inform the Director that a Customer is deceased in line with industry best practice so that the Customer experiences a seamless/sensitive journey with minimal effort.	
PPCL3-OPS-07	PPCL2-OPS-003	**Non-Digital Operational Processing**	The Supplier shall ensure that it is in line with the product sales terms and conditions so that they remain compliant as the Customer has agreed to the terms.	
PPCL3-OPS-08	PPCL2-OPS-003	**Non-Digital Operational Processing**	The Supplier shall reduce the number of warrants issued when a sale is not completed, so that the business can maintain the most possible cost effective service.	
PPCL3-OPS-09	PPCL2-OPS-003	**Non-Digital Operational Processing**	The Supplier shall ensure that a suitable ISA transfer 'in' process is in place so that Customer requests are effectively and efficiently dealt with in line with guidelines and timeframes and in line with the rest of the industry ISA Suppliers	
PPCL3-OPS-11	PPCL2-OPS-004	**Non-Digital Operational Processing**	The Supplier shall ensure that they manage maturing products to be able to comply with Customer instruction so that the Director is compliant against product terms and conditions and enables a seamless Customer journey.	
PPCL3-OPS-12	PPCL2-OPS-004	**Non-Digital Operational Processing**	The Supplier shall ensure that a suitable ISA transfer 'out' process is in place so that Customer requests are effectively and efficiently dealt with in line with the ISA guidelines and timeframes and in line with the rest of the industry ISA Suppliers	
PPCL3-OPS-13	PPCL2-OPS-004	**Non-Digital Operational Processing**	The Supplier shall ensure that Payments returned appear on the Faster Payments, BACS Returns and reject reports are resolved and updated on applicable systems so that Customer records are up to date and the business remains compliant against payments terms and conditions.	
PPCL3-OPS-14	PPCL2-OPS-004	**Non-Digital Operational Processing**	The Supplier shall ensure that Agents are able to manually key in payments (e.g. to make a goodwill payment, or to send a repayment via CHAPS rather than BACS as a result of our error) so that the Customer maintains a seamless Customer journey.	
PPCL3-OPS-15	PPCL2-OPS-004	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, provide the ability to initiate payments via CHAPS in exceptional circumstances as agreed with the Director so that the business maintains a efficient service.	
PPCL3-OPS-16	PPCL2-OPS-005	**Non-Digital Operational Processing**	The Supplier shall be able to deal with the Insolvency Service in relation to bankruptcy claims so that all claims are completed and all Customer records are updated in line with the agreed timelines.	
PPCL3-OPS-17	PPCL2-OPS-005	**Non-Digital Operational Processing**	The Supplier shall complete robust checks to ensure the appropriate proxy is identified so that the instruction or request is completed efficiently and effectively with minimal Customer and operational effort.	
PPCL3-OPS-18	PPCL2-OPS-006	**Non-Digital Operational Processing**	The Supplier shall work with the Director and other Suppliers to use the Directors tracing service and my lost account as per the BBA agreement to enable Customers to submit trace requests for potential the Director accounts and holdings, so that Customers can be reunited with potential historical funds	
PPCL3-OPS-19	PPCL2-OPS-007	**Non-Digital Operational Processing**	The Supplier shall be able to deal with correspondence that falls outside of proxies which are typically more complex, including but not limited to, family disputes, complex other process queries (such as sales, payments, tracing) so that the Customer experiences a seamless journey.	
PPCL3-OPS-20	PPCL2-OPS-007	**Non-Digital Operational Processing**	The Supplier shall capture and understand any actionable insight in order to suggest ways to minimise the amount of complex Customer correspondence within this workstream so that complex queries are reduced and Customers are then able to experience a seamless journey.	
PPCL3-OPS-21	PPCL2-OPS-008	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, update all Customer records associated with the Customer, when there has been a non digital change of details request, so that the Directors records and Customers details are kept up to date.	
PPCL3-OPS-22	PPCL2-OPS-008	**Non-Digital Operational Processing**	The Supplier shall provide a non digital service to complete more complex change of Customer details (e.g. Deed polls, gender transition) until the point that digital processing capability is provided so that the business is able to resolve Customer detail changes	

PPCL3-OPS-23	PPCL2-OPS-009	**Non-Digital Operational Processing**	The Supplier shall ensure the records management service can be accessed by all the other operational services to retrieve Customer data required so that the Customer can experience a seamless journey.	
PPCL3-OPS-24	PPCL2-OPS-010	**Non-Digital Operational Processing**	The Supplier shall provide operational processing that would inform the Director and other Suppliers of a Customers new address and details when the Supplier is informed of undelivered post so that the Customer records are kept up to date.	
PPCL3-OPS-25	PPCL2-OPS-010	**Non-Digital Operational Processing**	The Supplier to capture and understand any actionable insight to propose ways to minimise the amount of undeliverable mail so that Customer records are kept up to date.	
PPCL3-OPS-26	PPCL2-OPS-011	**Non-Digital Operational Processing**	The Supplier shall ensure identity documents can be requested and checked in line with industry standards so that Customer applications are processed in line with T&Cs.	
PPCL3-OPS-27	PPCL2-OPS-012	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers and the Director, enable the ability to issue numbers and passwords to non-digital Customers, so that these Customers can access the Directors digital and telephony services.	
PPCL3-OPS-28	PPCL2-OPS-013	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, enable the ability to re-issue numbers and new passwords to non digital Customers, so that these Customers can re-access the Directors digital and telephony services.	
PPCL3-OPS-29	PPCL2-OPS-014	**Non-Digital Operational Processing**	The Supplier shall ensure that back office staff are equipped and trained to execute operational processing on behalf of Customers who are unable to self serve so that the back office staff are able to support and assist with agents or Customer to complete their jobs to be done	
PPCL3-OPS-31	PPCL2-OPS-014	**Non-Digital Operational Processing**	The Supplier shall ensure that staff are able to support and encourage Customers to digitally self serve where able to so that the Customer is informed on how they can self-serve in the future to reduce the number of Customer interactions and transactions completed on behalf of the Customer	
PPCL3-OPS-33	PPCL2-OPS-014	**Non-Digital Operational Processing**	The Supplier shall ensure that the Customer receives the appropriate level of communication, which includes issuing communications at appropriate times throughout the Customer journey (trigger points as agreed with the Director) so that the number of interactions are reduced and the Customer experiences a seamless and efficient service.	
PPCL3-OPS-34	PPCL2-OPS-014	**Non-Digital Operational Processing**	The Supplier shall send Customer communications in line with the Directors' requirements and against agreed timelines (including adhoc requests / regular requests) so that Customers receive appropriate communications to enhance the Customers experience	
PPCL3-OPS-35	PPCL2-OPS-014	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with the Director, specify when communications are required aligned to agreed processes which do not require the Directors approval (included but not limited to annual statements) so that the business is able to operate as efficiently as possible.	
PPCL3-OPS-36	PPCL2-OPS-015	**Non-Digital Operational Processing**	The Supplier shall keep the Customer informed on where they are in the process so that the number of Customer interactions is minimised, the Customer experiences a seamless and efficient journey, and does not need to contact the Director.	
PPCL3-OPS-38	PPCL2-OPS-015	**Non-Digital Operational Processing**	The Supplier shall minimise the impact on the Customer of digital processes failing and moving to non-digital processes so that the Customer experiences a seamless journey.	
PPCL3-OPS-39	PPCL2-OPS-015	**Non-Digital Operational Processing**	The Supplier shall ensure that they have the ability to deal with any non-digital correspondence that comes from a British Forces Postal Offices (BFPO) address.	
PPCL3-OPS-40	PPCL2-OPS-015	**Non-Digital Operational Processing**	The Supplier shall ensure that any digital messaging that is in place across channels for Customers to support the completion of their 'jobs to be done' remains in place if the job drops out into non-digital processes, and before it goes back into digital processing so that the Customer has a consistent and seamless Customer journey.	
PPCL3-OPS-41	PPCL2-OPS-016	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, ensure that they are able to communicate and integrate with other Suppliers' systems in all forms as per final approved version of data sharing agreement(s) so that the business is able to operate effectively and has the necessary data, systems and applications to enable staff to support completion of the Customers end-to-end Customer journey (including Supplier to Customer and Customer back to Director)	
PPCL3-OPS-42	PPCL2-OPS-016	**Non-Digital Operational Processing**	The Supplier shall be able to communicate digitally with Customers that start their journey in the digital channel, but then drop into the non digital channel so that staff are able to serve Customers effectively and the Customer experiences a seamless journey	
PPCL3-OPS-43	PPCL2-OPS-016	**Non-Digital Operational Processing**	The Supplier shall be able to store a record of all Customer interactions (regardless of channel) between different Suppliers systems so that the Director can have an auditable trail of communications.	
PPCL3-OPS-44	PPCL2-OPS-017	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, ensure that they are able to communicate and integrate secure messaging with Customer contact case workflow management in all forms so that the business is able to operate effectively and has the necessary data, systems and applications to enable staff to support completion of the Customers end-to-end Customer journey (including Supplier to Customer and Customer back to Director)	
PPCL3-OPS-46	PPCL2-OPS-018	**Non-Digital Operational Processing**	The Supplier shall use Customer Personas through the process life-cycle, including but not limited to the point of design and any improvement activity, so that the Customer has a seamless journey for non-digital and digital processes.	
PPCL3-OPS-47	PPCL2-OPS-018	**Non-Digital Operational Processing**	The Supplier shall reduce non-digital Customer correspondence by encouraging the Customer to use digital channels where appropriate and not use non-digital channels so that the business remains effective and efficient	
PPCL3-OPS-48	PPCL2-OPS-019	**Non-Digital Operational Processing**	The Supplier shall identify such data requests (including, but not limited to Complaint, FOI and Data Subject) that fall in the non digital workflow and are sent on for appropriate processing, so that the Director can remain compliant and in conjunction with the Supplier can respond to the request in a timely manner.	
PPCL3-OPS-49	PPCL2-OPS-019	**Non-Digital Operational Processing**	The Supplier shall, in collaboration with other Suppliers, promptly provide data on request in all forms so that the Director can complete its obligations in a timely manner as required by the Director	
PPCL3-OPS-50	PPCL2-OPS-020	**Non-Digital Operational Processing**	The Supplier shall utilise the single and 2 way (B2C) secure messaging system in conjunction with other Suppliers (including Third Party Suppliers where applicable) so that staff can help carry out non digital transactions.	
PPCL3-OPS-51	PPCL2-OPS-020	**Non-Digital Operational Processing**	The Supplier shall work closely with other Suppliers to ensure that data, human errors and others incidents are resolved quickly so that the business maintains a safe and secure operation and is also in line with compliance (including and not limited to Data Protection legislation etc).	
PPCL3-OPS-52	PPCL2-OPS-021	**Non-Digital Operational Processing**	The Supplier shall automate processes where it is cost effective so that all Customer requirements are handled as efficiently as possible	
PPCL3-OPS-53	PPCL2-OPS-021	**Non-Digital Operational Processing**	The Supplier shall have the capability to review, improve, simplify, reduce volumes and processes as other Suppliers bring in more self serve ability so that Customer requests can be completed efficiently and effectively.	
PPCL3-OPS-54	PPCL2-OPS-021	**Non-Digital Operational Processing**	The Supplier shall ensure that there is an IT workflow system which shows the sub-process for each process identified (e.g. sub categories of General Correspondence) which can be displayed in an appropriate format so that the Director can complete oversight and assurance as required	
PPCL3-OPS-55	PPCL2-OPS-021	**Non-Digital Operational Processing**	The Supplier shall ensure that all processes implemented are future proof so that the business is able to adapt to changes at a time that it becomes feasible to automate.	
PPCL3-OPS-56	PPCL2-OPS-021	**Non-Digital Operational Processing**	The Supplier shall ensure that any non digital processes that cannot be automated are dealt with in the most efficient and effective way so that Customer requests are dealt with in a timely manner.	
PPCL3-OPS-57	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide a knowledge base / rules based workflow system for the operational staff so that cross process working is efficient and effective.	
PPCL3-OPS-58	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide the capability to provide non-digital services regardless of whether a digital solution is in place, to cater for those that are digitally excluded so that the Director can service all Customers.	
PPCL3-OPS-59	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure that all processes if dropped from digital to non-digital will be processed, including returning to digital methods, at the earliest opportunity so that the Customer experiences a seamless journey	
PPCL3-OPS-60	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall support the capability to reduce the fall out from digital and or assisted to non digital in agreement with the Director and collaboration with other Suppliers so that digital processes are the prioritised method of processing.	
PPCL3-OPS-61	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure that all staff are adequately trained to carry out all processes so that staff are able to efficiently and effectively deal with Customer requests	
PPCL3-OPS-62	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide an auditable quality assurance framework so that the Director can have oversight and assurance.	
PPCL3-OPS-63	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide an automated Quality Assurance process (e.g. an IT tool) so that the non-digital transactions processed can be validated or verified for their quality and accuracy	
PPCL3-OPS-64	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall, with the Director and other Suppliers, provide inputs to the forecasting process to adequately resource non-digital operations so that Customer requests can be processed within timescales	

PPCL3-OPS-65	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier in collaboration with Other Suppliers shall provide the necessary data for dashboards which shows details (e.g. headcount, holdovers etc) that help show the service performance and which help to prevent any resource gaps or any issues so that the business is able to run an effective and seamless service for the Customer	
PPCL3-OPS-66	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall present further opportunities to automate service processes and share with the Director so that the business can respond and resolve Customer requests and claims in the most efficient way.	
PPCL3-OPS-67	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall present ways to automate and improve the Operational Processing so that where there is a cost effective method the Supplier is able to implement an automated service	
PPCL3-OPS-69	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure they have suitable exception handling capability across all services so that non digital Customer requests and queries can be completed with minimal Customer and operational effort.	
PPCL3-OPS-70	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure that procedures and including the associated documented procedures are regularly reviewed so that staff follow the most up to date procedures as required.	
PPCL3-OPS-72	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall have a Operations wide skills matrix across the various Supplier services and processes that will be in place so that the business can ensure that it has the relevant skills in the business to operate effectively	
PPCL3-OPS-73	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide the recruitment, management and development of all appropriately skilled staff required for the delivery of non-digital processing services so that the business is able to provide an effective service across all services and sub-processes	
PPCL3-OPS-74	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall have an efficient security checking process (in line with the Director security requirements) for any new starters so that recruits are highly productive and quickly effective to manage Customers	
PPCL3-OPS-75	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure non digitised processes are aligned to the agreed KPIs so that it meets the minimum requirements to respond to the Customer within timescales	
PPCL3-OPS-76	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall, where applicable to non-digital processing service requirements and scope, support and/or deliver the following activities including but not limited to: • Assurance and oversight activity; • Complaints procedures & complaints handling; • Analytics and Insights; • Freedom of Information requirements; • Subject Access Requests; • Fraud/suspicious activity prevention and reporting; • Auditing check and assessments; • Change Request management and implementation; • Contract Management; • Training; • Incident reporting and resolution; • Resolution planning; and • Issue identification, root cause analysis, escalation and remediation.	
PPCL3-OPS-87	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall create and administer an SEO blocking process so that sales are correct and the new premium bonds are entered into the appropriate prize draw	
PPCL3-OPS-88	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall process financial advisor paper communications as required (until the point its digitised) so that the business can maintain a seamless journey for Financial Advisors	
PPCL3-OPS-89	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall create and administer an SEO blocking process so that sales and evidence of identity are correct and the new premium bonds are entered into the appropriate prize draw	
PPCL3-OPS-90	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide the ability for their operational teams to contribute to, and be involved in, continuous improvement/CX/Test & Learn activity so that the end-to-end services and processes can continually be improved	
PPCL3-OPS-91	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure that the Director is able to contribute to continuous improvement /CX/Test & Learn activities so that the end-to-end services and processes can be continually improved and the Director has oversight and assurance	
PPCL3-OPS-92	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure the Director has access to the necessary non-digital systems so that the Director has clear independent visibility of all contacts and performance MI (real-time and historical), reasons for contact and can assure the service.	
PPCL3-OPS-93	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall collaborate with Other Suppliers to ensure that access to systems and data is available as required so that all staff have the tools required to perform their role.	
PPCL3-OPS-94	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall ensure that the Director has access to procedures and associated documentation so that oversight and assurance can be completed	
PPCL3-OPS-95	PPCL2-OPS-022	**Non-Digital Operational Processing**	The Supplier shall provide a system that delivers suitable compliance training for its staff with supporting MI so that the Director can validate results and assure the Suppliers staff are adequately trained.	
PPCL3-PD-001	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall work with the Director to create a Jackpot winner service that aligns with the Directors brand and customer experience principles, so that customer has a positive and supportive experience	
PPCL3-PD-002	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall collaborate with the Directors to develop training procedures for the jackpot prize, so that the operations are aligned with the Directors brand and experience principles	
PPCL3-PD-003	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall ensure the winner of the jackpot prize and the nominated bank details are verified so that the prize payment is made to the correct customer	
PPCL3-PD-004	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall contact the jackpot winners after verification, one day prior to the result day, so that payment can be made on the specified date, as agreed by the Director	
PPCL3-PD-005	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall ensure there is an agreed process to contact overseas jackpot winners so that there is a positive customer and brand experience for delivery of the jackpot prizes	
PPCL3-PD-006	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall ensure that that the jackpot winner has complete anonymity so that the customers identity is protected	
PPCL3-PD-007	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall provide an Agent Million team so that there is a positive customer and brand experience for delivery of the jackpot prizes	
PPCL3-PD-008	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall allow the Directors to attend the Agent Million visit to the customer, as requested, so that the Directors can ensure the customer and brand experience is positive and aligned to the agreed operating procedures	
PPCL3-PD-009	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall provide information to the winning customer, confirming the win and details of the next steps, in line with the Directors brand and experience principles, so that the customer is correctly informed of the prize and its terms and conditions, whilst maintaining a consistent and positive experience.	
PPCL3-PD-010	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall support the jackpot winner with post winning queries so that customers can make a decision on where the funds will be paid to, as agreed with the Director	
PPCL3-PD-011	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall notify Other Suppliers when electronic payment is required so that the payments are made as per the customers preference	
PPCL3-PD-012	PPCL2-PD-002	**Non-Digital Prize Draw**	The Supplier shall arrange the warrant payment if chosen by the customer, collaborating with the Core Banking supplier, so that payments are made as per the customers preference	
PPCL3-PD-013	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall only issue warrants upon request of high value prize winning customers, so that payment is made securely to the prize winning customer only	
PPCL3-PD-014	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall collaborate with other operational teams to deal with queries and processes relating to the Prize Draw System and High Value Prizes, so that customer queries or requests can be answered	
PPCL3-PD-015	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall provide a team with training and access, to support the operational processing of the Prize Draw and delivery of high value prizes, so that the integrity of the prize draw can be maintained	
PPCL3-PD-016	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall provide a team with training and access, to support the operational processing of customer queries, so that the customer experience is positive	
PPCL3-PD-017	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall ensure that the Director is able to complete various assurance and oversight activities across the Prize Draw process, as and when required, including (but not limited to) the generation of the prize draw, processing of high value prizes and responses to customer queries, so that the Director can conduct prize draw assurance, ensuring all parties are confident the Prize Draw process works as designed	
PPCL3-PD-018	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall provide operational processing related to Missed Opportunities in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with Other Suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL3-PD-019	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall provide operational processing for the manual services related to Reserve Prizes in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with Other Suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	

PPCL3-PD-020	PPCL2-PD-003	**Non-Digital Prize Draw**	The Supplier shall provide operational processing for the manual services related to Excess Refund Processing in the Premium Bond holdings and/or the Prize Draw process, until such a point and in collaboration with Other Suppliers, the services have been digitised, so that customer journeys can be completed with minimal customer and operational effort.	
PPCL3-PD-021	PPCL2-PD-007	**Non-Digital Prize Draw**	The Supplier shall notify Other Suppliers of permitted blockings, for agreed upon scenarios within the Prize Draw process, so that customer accounts and records are protected	
PPCL3-PD-022	PPCL2-PD-007	**Non-Digital Prize Draw**	The Supplier shall ensure the Prize Draw team makes updates to the master customer record as part of the Prize Draw Process, where required, so that the customer records are kept up to date and the integrity of the draw is not compromised	
PPCL3-PD-023	PPCL2-PD-008	**Non-Digital Prize Draw**	The Supplier shall alert Other Suppliers of warrants being issued, where needed, so that the end to end process of prize payment is completed correctly	
PPCL3-PD-024	PPCL2-PD-008	**Non-Digital Prize Draw**	The Supplier shall check the validity of the high value prize claim form, if not done digitally, alerting Other Suppliers if successfully validated, so that the Director can award the prize	
PPCL3-PD-025	PPCL2-PD-008	**Non-Digital Prize Draw**	The Supplier shall collaborate with the Director and Other Suppliers to support the automated and digital self-service activities so that the Director can reduce risks and maximise the efficiency of the prize draw.	
PPCL3-RC-001	PPCL2-RC-001	**Risk**	The Supplier shall operate a risk management framework for the services delivered, based on a 3-lines of defence model. The framework shall be aligned to the Director's framework, so that the Director is able to align frameworks used across Suppliers.	
PPCL3-RC-002	PPCL2-RC-001	**Risk**	The Supplier shall adopt a risk taxonomy, risk methodologies, risk assessment matrix which is aligned to the Director's guidance / templates.	
PPCL3-RC-003	PPCL2-RC-001	**Risk**	The Supplier's Risk Function will be headed by an individual with the appropriate level of seniority within the Supplier's organisation to make decisions on resource allocation and the management of risk. They will provide independence and will also have accountability to the Account Director.	
PPCL3-RC-004	PPCL2-RC-001	**Risk**	The Supplier shall have an established and documented appetite for risk that aligns with the appetite for risk set out by the Director.	
PPCL3-RC-005	PPCL2-RC-002	**Risk**	The Supplier must provide data to the scope, format and frequency required by the Director to enable integration with the enterprise risk tooling operated by the Director and deliver it to the Director's risk function, to facilitate a view of risk exposures across the whole enterprise via a single interface. Examples of Risk data include but are not limited to: *Key risks and controls, *Performance data *Key risk and control indicators, *Forecasts and future projections, *Open audit actions and progress on remediation, *New and Open breaches, incidents & losses, including trends, themes and progress on remediation, *Planned changes, including progress on implementation, *Results of control testing (such as RCSA and audit / assurance activity), *Actions and timescales to address risk exposures that are outside of appetite	
PPCL3-RC-006	PPCL2-RC-002	**Risk**	The Supplier shall perform regular analysis on risk data of services supplied. Analysis shall support interpretation of raw data, to be presented to the Director.	
PPCL3-RC-007	PPCL2-RC-003	**Risk**	The Supplier shall make available to the Director upon request resources to support any Director-driven audits/inspections. Resources include but are not limited to: *all information requested by the Director within the permitted scope of the audit; *books and records; *access to any sites controlled by the Supplier and to any equipment used (whether exclusively or non-exclusively) in the performance of the services provided; *Supplier personnel; *a suitable working environment for the Director and/or the Director's representatives where an on-site presence is required. Note, notice will be given by the Director before embarking on an audit/inspection.	
PPCL3-RC-008	PPCL2-RC-003	**Risk**	The Supplier shall have established Quality Assurance and Internal Audit functions which the Director has the right to inspect / get data from.	
PPCL3-RC-009	PPCL2-RC-003	**Risk**	The Supplier's assurance/internal audit functions shall provide a point of contact to engage in the Director's Audit governance activities, including: *attendance at regular the Director's Audit meetings and committees, *providing reporting and updates to the Director on Audit related matters.	
PPCL3-RC-010	PPCL2-RC-003	**Risk**	The Supplier shall support the Director's annual audit programme (as applicable) by undertaking activities such as: *attending meetings to discuss strategic objectives, *providing information on key Risk issues and changes to people, systems and processes, *providing quarterly internal audit plans *providing monthly updates to the status of prior audit recommendations.	
PPCL3-RC-011	PPCL2-RC-003	**Risk**	The Supplier shall attend the Director's Audit governance e.g. Audit Committee when required and input any relevant materials / reporting prior to the meeting.	
PPCL3-RC-012	PPCL2-RC-003	**Risk**	The Supplier shall meet with the Director no fewer than four (4) times per annum, at the Director's invitation to discuss the effectiveness of the Risk Management Framework and assurance monitoring.	
PPC-L3-SEC-001	PPCL2-SEC-001	**Security**	The Supplier shall comply with all of the Director's security policies, standards and any applicable procedures or guidelines.	The Supplier shall comply with all of the Director's security policies
PPC-L3-SEC-002	PPCL2-SEC-001	**Security**	The Supplier shall comply with the current HMG Security Policy Framework, the HMG Security Classifications for Information Assets, and all current HMG Security Standards.	The Supplier shall comply with all current HMG Security Standards
PPC-L3-SEC-003	PPCL2-SEC-001	**Security**	The Supplier shall comply with the current NIST Cybersecurity Framework	
PPC-L3-SEC-004	PPCL2-SEC-001	**Security**	The Supplier must achieve Maturity Level 4 in NIST PRISMA reviews	
PPC-L3-SEC-005	PPCL2-SEC-001	**Security**	The Supplier will be subject to an annual review of their NIST PRISMA level. This will be undertaken by a 3rd party and shall be agreed by the Director. Such reviews will be at the Supplier's cost.	
PPC-L3-SEC-006	PPCL2-SEC-001	**Security**	The Supplier shall provide access to the Supplier Personnel responsible for security and information assurance	
PPC-L3-SEC-007	PPCL2-SEC-001	**Security**	The Supplier shall implement its own internal cyber security risk management approach, which shall be compliant with the provisions of this Schedule 2.4 and the Statement of Information Risk Appetite.	
PPC-L3-SEC-008	PPCL2-SEC-001	**Security**	The Supplier shall coordinate its internal cyber security risk management activities with the overall approach to cyber security risk management across the Wider Information Management System, as directed by the Director.	
PPC-L3-SEC-009	PPCL2-SEC-001	**Security**	The Supplier shall provide the Security Governance Forum with access to a high-quality, simple and timely management information report relating to cyber resilience and security, as reasonably requested by the Director	
PPC-L3-SEC-010	PPCL2-SEC-001	**Security**	The Supplier shall implement a cyber-resilience strategy that aligns to the Directors Statement of Information Risk Appetite.	
PPC-L3-SEC-011	PPCL2-SEC-001	**Security**	The Supplier recognises that the need for the Core Information Management System and the Director as a whole, to comply with applicable regulation and guidance may require coordination of the approach to implementing cyber security systems across the Core Information Management System and Wider Information Management System. In such circumstances, the Supplier shall follow the guidance of the Director in ensuring overall compliance.	
PPC-L3-SEC-012	PPCL2-SEC-001	**Security**	The Supplier shall ensure, at all times during the Term, that the entirety of the CIMS (whether provided by the Supplier or CIMS Sub-contractors) is certified as compliant with: *ISO/IEC 27001:2013 by a United Kingdom Accreditation Service (UKAS) *approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and *7.1.2 Cyber Essentials Plus, in all respects applicable to the Services, and it shall provide the Director with a copy of each such certificate of compliance before the Supplier and/or any CIMS Sub-contractor shall be permitted to use the Core Information Management System to receive or Process Director Data.	
PPC-L3-SEC-013	PPCL2-SEC-001	**Security**	The Supplier shall ensure its leadership's commitment to and support of cyber security, information security and risk management to protect the Director against such exposures. It shall appoint individuals at the relevant level with the relevant skill and experience to discharge their duties.	
PPC-L3-SEC-014	PPCL2-SEC-001	**Security**	The Supplier shall perform checks to ensure the ongoing compliance of the CIMS with assured security patterns and designs, highlighting any non-compliance as a security incident, and account for overall compliance status to the security forum on a monthly basis.	

PPC-L3-SEC-015	PPCL2-SEC-001	**Security**	To facilitate Assurance of the Core Information Management System, the Supplier shall provide the Director and its authorised representatives with: *Access to the Sites, Supplier Staff and/or their vetting records, ICT information assets and ICT systems within the Core Information Management System on request (except where explicitly agreed by the Director that this is not applicable for specific cloud services); and *Any other information and/or documentation that the Director or its authorised representatives may reasonably require, to enable the Director to establish that the Core Information Management System is compliant with the Security Management Plan.	To facilitate Assurance of the Core Information Management System, the Supplier shall provide the Director and its authorised representatives with: *Access to the Sites, Supplier Staff and/or their vetting records, ICT information assets and ICT systems within the Core Information Management System on request; and *Any other information and/or documentation that the Director or its authorised representatives may reasonably require, to enable the Director to establish that the Core Information Management System is compliant with the Security Management Plan.
PPC-L3-SEC-016	PPCL2-SEC-001	**Security**	The Supplier shall maintain an inventory of physical and virtual devices used to provide the CIMS (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall maintain an inventory of physical and virtual devices used to provide the CIMS.
PPC-L3-SEC-017	PPCL2-SEC-001	**Security**	The Supplier shall maintain an inventory of software platforms, applications and external services used to provide the CIMS	
PPC-L3-SEC-018	PPCL2-SEC-001	**Security**	The Supplier shall ensure that no unauthorised devices are permitted to connect to the network without security authorisation.	
PPC-L3-SEC-019	PPCL2-SEC-001	**Security**	The Supplier shall maintain an inventory of all supported interorganisational communication and data flows across the Customer Contact and Operations Layer, including those using the Integration Platform.	
PPC-L3-SEC-020	PPCL2-SEC-001	**Security**	The Supplier shall implement, and only implement, interorganisational data and communication flows that have been agreed by the Director through an Enterprise Architecture process.	
PPC-L3-SEC-021	PPCL2-SEC-001	**Security**	The Supplier shall catalogue external information systems accessed by the CIMS.	
PPC-L3-SEC-022	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the data, personnel, devices, systems, and facilities that make up the CIMS are identified and managed consistent with the likelihood that their compromise could breach the tolerances within the Statement of Information Risk Appetite.	
PPC-L3-SEC-023	PPCL2-SEC-001	**Security**	All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services, and shall repeat checks according to the Directors policy.	
PPC-L3-SEC-024	PPCL2-SEC-001	**Security**	Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard (or any future replacement thereof) including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. Supplier Staff located outside the UK shall only be involved in the management and/or provision of the Services where the Director has expressly agreed in writing and equivalent local standards for pre-employed checks shall be used, as agreed with the Director.	Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard (or any future replacement thereof) including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
PPC-L3-SEC-025	PPCL2-SEC-001	**Security**	The Director and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Director to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Security Check or any future replacement thereof), and shall implement and maintain these checks. Roles which are likely to require a specific national security vetting clearance include: - Provider Personnel with Enhanced Privileges (root, system administrator, database administrator or equivalent); - Provider Personnel with access to live Bulk Customer Data or copies of the live Bulk Customer Data; - Provider Personnel working in an information security role or with responsibility for managing information security personnel; - Provider Personnel working in a financial crime role where those individuals have access to details relating to criminal investigations or with responsibility for managing financial crime personnel; and - Provider Personnel roles with non-administrative/privileged access to Bulk Customer Data where: *access is to full copies of live Bulk Customer Data that allows individuals to be identified; *access is not being controlled by the application to single records only; and *no audit trail of access to information records is created.	
PPC-L3-SEC-026	PPCL2-SEC-001	**Security**	The Supplier shall not permit Supplier Staff who fail the security checks to be involved in the management and/or provision of the Services except where the Director has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.	
PPC-L3-SEC-027	PPCL2-SEC-001	**Security**	The Supplier shall adapt and continuously improve cyber resilience measures based on the Directors Statement of Information Risk Appetite.	
PPC-L3-SEC-028	PPCL2-SEC-001	**Security**	The Supplier shall communicate its dependency on other Suppliers to deliver the service (whether part of the WIMS or the Supplier's supply chain), as a component of its security reporting to the Director.	
PPC-L3-SEC-029	PPCL2-SEC-001	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall identify dependencies and critical functions/Important Business Services for delivery of the services and ensure they are subject to business continuity and operational resilience plans	
PPC-L3-SEC-030	PPCL2-SEC-001	**Security**	The Supplier shall pro-actively scan the Core Information Management System for vulnerable components and address discovered Vulnerabilities through the processes described in the Security Management Plan	
PPC-L3-SEC-031	PPCL2-SEC-001	**Security**	The Supplier shall notify the Director within 2 Working Days after becoming aware of a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;	
PPC-L3-SEC-032	PPCL2-SEC-001	**Security**	The Supplier shall prepare and submit to the Director documentation of the security risk management processes for the Core Information Management System, which shall be subject to reviewed by the Director, and shall subsequently manage security in accordance with the Security Management Plan	
PPC-L3-SEC-033	PPCL2-SEC-001	**Security**	The Security Management Plan shall reflect security risk management approaches that are informed by the Directors provided Risk Appetite.	
PPC-L3-SEC-034	PPCL2-SEC-001	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall produce and prepare for implementation of disaster recovery and business continuity plans that covers how service provision will continue during an unplanned disruption in service.	
PPC-L3-SEC-035	PPCL2-SEC-001	**Security (Business Continuity/ Disaster Recovery)**	The Supplier's business continuity plan shall define shared services that could in the event of an incident impact them and their peers. Controls must be implemented to allow service provision to continue in the event that an incident occurs due to highly concentrated services or capabilities.	
PPC-L3-SEC-036	PPCL2-SEC-001	**Security**	The Supplier shall identify, assess, and prioritise Other Suppliers and third-party partners of information systems, components, and services using a cyber supply chain risk assessment process	
PPC-L3-SEC-037	PPCL2-SEC-001	**Security**	The Supplier shall ensure that any use of subcontractors to deliver the services is in accordance with these security requirements and schedule 2.4	
PPC-L3-SEC-038	PPCL2-SEC-001	**Security**	The Supplier shall submit evidence for review at the security governance forum to demonstrate that they are meeting their obligations as stated in the Security Management Plan, including being subject to, and/or conducting tests and audits on request by the Director.	
PPC-L3-SEC-039	PPCL2-SEC-001	**Security (Business Continuity/ Disaster Recovery)**	The Supplier will plan its approach to response and recovery from business continuity and disaster recovery events across the supply chain, and test these plans on an annual basis	
PPC-L3-SEC-040	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes	
PPC-L3-SEC-041	PPCL2-SEC-001	**Security**	The Supplier shall ensure that physical access to assets and the sites from which services are delivered is managed and protected, and limited to identified, authorised and authenticated personnel	
PPC-L3-SEC-042	PPCL2-SEC-001	**Security**	The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Director on request (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Director on request
PPC-L3-SEC-043	PPCL2-SEC-001	**Security**	The Supplier shall ensure that services are delivered from locations which are assessed and approved for compliance to ISO27001 and HMG standards	
PPC-L3-SEC-044	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Remote access to the CIMS is securely managed using multifactor authentication and performed in a manner that prevents unauthorised access	
PPC-L3-SEC-045	PPCL2-SEC-001	**Security**	The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites, using role-based access controls, so that such persons are allowed access only to those parts of the Sites and the Supplier System they require, and the principle of separation of duties is applied.	
PPC-L3-SEC-046	PPCL2-SEC-001	**Security**	The Supplier shall maintain a process to identify and promptly revoke access permissions where no longer required and shall conduct a monthly review of the results of this process.	
PPC-L3-SEC-047	PPCL2-SEC-001	**Security**	The Supplier shall revoke access rights of leavers immediately on the last day of employment.	
PPC-L3-SEC-048	PPCL2-SEC-001	**Security**	The Supplier shall implement boundary and internal protections to prevent unauthorised access to the CIMS.	
PPC-L3-SEC-049	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the CIMS shall only directly interact with the WIMS via the Integration Platform, except where explicitly agreed with the Director.	
PPC-L3-SEC-050	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Identities are proofed and bound to credentials and asserted in interactions.	
PPC-L3-SEC-051	PPCL2-SEC-001	**Security**	The Supplier shall ensure that all users, hardware, software and system components of the CIMS are authenticated before accessing the CIMS.	The Supplier shall ensure that all users, hardware and software components of the CIMS are authenticated before accessing the CIMS.

PPC-L3-SEC-052	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Director's data receive regular security training, applicable to their roles, that reflects the degree of access those individuals have to the Sites, the IT Environment or the Directors Data.	The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Director's data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Directors Data.
PPC-L3-SEC-053	PPCL2-SEC-001	**Security**	The Supplier shall ensure, and shall conduct and report to the Director periodic assurance activities to verify that: *appropriate physical security measures are in place; *cyber security staff and privileged users understand their roles and responsibilities.	
PPC-L3-SEC-054	PPCL2-SEC-001	**Security**	The Supplier shall communicate security roles and responsibilities to its Other Suppliers and partners.	
PPC-L3-SEC-055	PPCL2-SEC-001	**Security**	The Supplier shall protect the confidentiality, integrity and availability of Director data and ensure it is encrypted in transit and at rest.	
PPC-L3-SEC-056	PPCL2-SEC-001	**Security**	The Supplier shall manage and evidence the removal, transfer and secure disposal of data including hardware assets which it is stored upon (except where explicitly agreed by the Director that this is not applicable for specific cloud services), implementing a data destruction policy provided by the Director	The Supplier shall manage and evidence the removal, transfer and secure disposal of data including hardware assets which it is stored upon, implementing a data destruction policy provided by the Director
PPC-L3-SEC-057	PPCL2-SEC-001	**Security**	The Supplier shall Provide adequate storage capacity to maintain the availability of all required Director Data.	
PPC-L3-SEC-058	PPCL2-SEC-001	**Security**	The Supplier shall implement data leakage protections for all Director Data	
PPC-L3-SEC-059	PPCL2-SEC-001	**Security**	The Supplier shall ensure the integrity of software, firmware, Director Data and information necessary to provide the services	
PPC-L3-SEC-060	PPCL2-SEC-001	**Security**	The Supplier shall ensure that personally identifiable information is not processed or stored for non-production purposes. Any processing or storage of personal data for non-production purposes must use synthetic data, or anonymised/pseudonymised versions of live data that have been approved by the Director.	
PPC-L3-SEC-061	PPCL2-SEC-001	**Security**	The Supplier shall ensure that non-production environments, including development and testing environments, are segregated from production environments and from each other.	
PPC-L3-SEC-062	PPCL2-SEC-001	**Security**	The Supplier shall ensure that all hardware used in the delivery of services to the Director includes integrity checking mechanisms to verify hardware integrity (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall ensure that all hardware used in the delivery of services to the Director includes integrity checking mechanisms to verify hardware integrity.
PPC-L3-SEC-063	PPCL2-SEC-001	**Security**	The Supplier shall maintain and be accountable for the secure configuration of IT within the CIMS.	
PPC-L3-SEC-064	PPCL2-SEC-001	**Security**	The Supplier shall create and maintain baseline configurations of IT within the CIMS ensuring that the concept of least functionality is adopted and that current patch levels are implemented at all times	
PPC-L3-SEC-065	PPCL2-SEC-001	**Security**	The Supplier shall operate a secure development process that ensures security and privacy are addressed by design for all IT within the CIMS	
PPC-L3-SEC-066	PPCL2-SEC-001	**Security**	The Supplier shall conduct an IT Health Check prior to the implementation of any change to the CIMS deemed to impact security, unless an exemption is agreed with the Director	
PPC-L3-SEC-067	PPCL2-SEC-001	**Security**	The Supplier shall manage and provide evidence for a controlled process of configuration change, which shall include undertaking a risk assessment to assess the impact of such change on security.	
PPC-L3-SEC-068	PPCL2-SEC-001	**Security**	The Supplier shall back-up Director Data to recover all data up to the point of a data loss event, ensuring all backups are free from malicious software and encrypted.	
PPC-L3-SEC-069	PPCL2-SEC-001	**Security**	The Supplier shall provide a tested capability to recover data after a data loss event within 2 hours and shall validate that the back-ups are free from malicious software (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall provide a tested capability to recover data after a data loss event within 2 hours and shall validate that the back-ups are free from malicious software.
PPC-L3-SEC-070	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the Director's policy and regulations for the physical operating environment are met (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall ensure that the Director's policy and regulations for the physical operating environment are met
PPC-L3-SEC-071	PPCL2-SEC-001	**Security**	All Director data must be destroyed in line with the Director's data destruction policy and evidence of this supplied to the Director for assurance (except where explicitly agreed by the Director that this is not applicable for specific cloud services)	All Director data must be destroyed in line with the Director's data destruction policy and evidence of this supplied to the Director for assurance
PPC-L3-SEC-072	PPCL2-SEC-001	**Security**	The Supplier shall conduct a quarterly continuous improvement review of information protection processes, agreeing any recommendations with the Director and implementing those recommendations.	
PPC-L3-SEC-073	PPCL2-SEC-001	**Security**	The Supplier shall report on a monthly basis to the Director on: I) the number of cases where security and information protection controls prevent compromise of information ii) the number of cases where security and information protection controls circumvention has been identified or iii) where security and information protection controls have been identified as providing an obstacle to use of the CIMS or delivery of the services.	
PPC-L3-SEC-074	PPCL2-SEC-001	**Security**	The Supplier shall ensure that cyber security is addressed by human resources practices including skills management, recruitment, termination and disciplinary practices.	
PPC-L3-SEC-075	PPCL2-SEC-001	**Security**	The Supplier shall produce a formal Vulnerability Management plan, addressing the approach to detecting and remedying Vulnerabilities.	
PPC-L3-SEC-076	PPCL2-SEC-001	**Security**	The Supplier shall provide to the Director a monthly report on the presence of all publicly disclosed Vulnerabilities, or those notified by the Director, affecting systems directly involved in the delivery of the Services.	
PPC-L3-SEC-077	PPCL2-SEC-001	**Security**	For Vulnerabilities with a CVSS score of 7 or higher (as described at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) or higher and/or those described by the software provider as HIGH RISK or CRITICAL, the Supplier shall notify the Director within 48 hours of disclosure.	
PPC-L3-SEC-078	PPCL2-SEC-001	**Security**	For Vulnerabilities with a CVSS score of 5-7, the Supplier shall notify the Director within 5 Working Days of disclosure.	
PPC-L3-SEC-079	PPCL2-SEC-001	**Security**	Where vulnerabilities are disclosed by software providers (where CVSS do not provide a score) and that software is used to provide services to the Director within the CIMS the severity rankings shall be mapped to CVSS scores for the purpose of notifying the Director. (For example, Microsoft use the terms Critical, Important, Moderate and Low. The Director views Critical and Important to map to a CVSS score of 7 or higher. Moderate equates to a CVSS of between 5-7. Low would equate to <5).	
PPC-L3-SEC-080	PPCL2-SEC-001	**Security**	The Supplier shall ensure that any vulnerabilities affecting services provided to the Director shall be mitigated: - Within 5 days of discovery for Vulnerabilities with an actual or deemed CVSS score of 7 or higher - Within 2 weeks for Vulnerabilities with an actual or deemed CVSS score of 5-7 - Other vulnerabilities shall be scheduled for mitigation in a future release with any delay beyond 6 weeks to be agreed with the Director.	
PPC-L3-SEC-081	PPCL2-SEC-001	**Security**	The Supplier shall perform and log maintenance and repair of all assets providing services within the CIMS (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall perform and log maintenance and repair of all assets providing services within the CIMS
PPC-L3-SEC-082	PPCL2-SEC-001	**Security**	The Supplier shall ensure that maintenance of all assets is approved, logged, and performed in a manner that prevents unauthorised access and abuse of administrative access (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall ensure that maintenance of all assets is approved, logged, and performed in a manner that prevents unauthorised access and abuse of administrative access
PPC-L3-SEC-083	PPCL2-SEC-001	**Security**	The Supplier shall ensure that any device which is used to Process Director Data meets all of the security requirements set out in the current NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.	
PPC-L3-SEC-084	PPCL2-SEC-001	**Security**	The Supplier shall incorporate the principle of least functionality by configuring systems to provide only essential capabilities and disabling unnecessary services.	
PPC-L3-SEC-085	PPCL2-SEC-001	**Security**	The Supplier shall ensure that all Supplier access (e.g. for configuration, administration and maintenance) to IT systems provided to the Director must be undertaken with appropriate security controls in place to ensure the Confidentiality, Integrity and Availability of the CIMS.	
PPC-L3-SEC-086	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the entire IT infrastructure supporting the CIMS is protected by current Anti-Malicious Software which checks for, prevents the introduction of, and contains the spread and impact of Malicious Software	
PPC-L3-SEC-087	PPCL2-SEC-001	**Security**	The Supplier shall conduct Vulnerability scanning and assessments of the Core Information Management System monthly (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall conduct Vulnerability scanning and assessments of the Core Information Management System monthly
PPC-L3-SEC-088	PPCL2-SEC-001	**Security**	The Supplier shall continuously improve its security management plan and security control environment, agreeing any changes with the Director	
PPC-L3-SEC-089	PPCL2-SEC-001	**Security**	The Supplier will ensure they have access to HMG and financial services industry specific sources of information relating to events, risks and best practice.	
PPC-L3-SEC-090	PPCL2-SEC-001	**Security**	The Supplier shall support the Director's requirements as a public sector body by implementing security solutions offered by NCSC as part of the Active Cyber Defence programme (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall support the Director's requirements as a public sector body by implementing security solutions offered by NCSC as part of the Active Cyber Defence programme.
PPC-L3-SEC-091	PPCL2-SEC-001	**Security**	The Supplier shall utilise the Cyber Security Information Sharing Partnership (CiSP) and ensure that relevant information relating to security threats are assessed; where additional security controls requirements are identified they shall be implemented to mitigate such threats.	
PPC-L3-SEC-092	PPCL2-SEC-001	**Security**	The Supplier shall scan for vulnerabilities against the US National Vulnerability Database (except where explicitly agreed by the Director that this is not applicable for specific cloud services).	The Supplier shall scan for vulnerabilities against the US National Vulnerability Database
PPC-L3-SEC-093	PPCL2-SEC-001	**Security**	The Supplier shall train Board members in cyber security, the material for which should include, but will not be limited to, the NCSC Board Toolkit as a resource to assist with such training.	

PPC-L3-SEC-094	PPCL2-SEC-001	**Security**	The Supplier shall ensure that where has made use of, or relies on, open-source code/API's or similar, that a robust and repeatable process is documented and followed to validate the provenance and content of such code to assure the Director that no vulnerabilities are identified and introduced to the CIMS	
PPC-L3-SEC-095	PPCL2-SEC-001	**Security**	The Supplier should ensure that on at least an annual basis they validate their control environment against the NCSC 10 Steps to Cyber Security and provide a copy to the Director for assurance.	
PPC-L3-SEC-096	PPCL2-SEC-001	**Security**	The Supplier shall ensure that it undertakes at least annual cyber security testing of its people, processes, systems and environments and provide a report of the activities and outcomes to the Director.	
PPC-L3-SEC-097	PPCL2-SEC-001	**Security**	The Supplier shall ensure that code held in escrow is encrypted and a process of validation is undertaken to ensure that the code is free from vulnerabilities and malicious software.	
PPC-L3-SEC-098	PPCL2-SEC-001	**Security**	The Supplier shall provide the Director and the CSMS (Central Security Monitoring Service) with the inventory of all assets used to provide the CIMS, where prescribed by the Director, on a monthly basis. (assets include all hardware, software, software platforms, operating systems, external services & applications).	The Supplier shall provide the Director and the CSMS (Central Security Monitoring Service) with the inventory of assets used to provide the CIMS on a monthly basis. (assets include all hardware, software, software platforms, operating systems, external services & applications).
PPC-L3-SEC-099	PPCL2-SEC-001	**Security**	The Supplier shall ensure all assets within the scope of the CIMS are monitored, and where prescribed by the Director, monitoring is conducted in accordance with the instructions of the CSMS (Central Security Monitoring Service).	The Supplier shall ensure all assets within the scope of the CIMS are monitored in accordance with the instructions of the CSMS (Central Security Monitoring Service).
PPC-L3-SEC-100	PPCL2-SEC-001	**Security**	The Supplier shall subscribe to authoritative sources of Threat Intelligence and implement a mechanism for timely review, analysis and action resulting from Threat Intelligence received from these sources or sources to which the Director provides access.	
PPC-L3-SEC-101	PPCL2-SEC-001	**Security**	The Supplier shall also ensure that they have access to published sources of Threat Intelligence selected to be relevant to the services provided.	
PPC-L3-SEC-102	PPCL2-SEC-001	**Security**	The Supplier shall identify, document and communicate to the Director any Threats identified in the analysis of Threat Intelligence that are relevant to the services.	
PPC-L3-SEC-103	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Threat Intelligence received from sources is provided to the CSMS (Central Security Monitoring service).	
PPC-L3-SEC-104	PPCL2-SEC-001	**Security**	Requirement removed (duplicate of PPC-L3-SEC-019)	The Supplier shall maintain an inventory of all supported interorganisational communication and data flows across the Contact Centre and Operations, including those using the Integration Platform.
PPC-L3-SEC-105	PPCL2-SEC-001	**Security**	The Supplier shall inform the Director and the CSMS as soon as possible, but in any case, within 24 hours, when it becomes aware of any new Threat, Vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System, collaborating to identify potential business impacts and likelihoods.	
PPC-L3-SEC-106	PPCL2-SEC-001	**Security**	Where the Supplier becomes aware of any new Threat, Vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System it shall select and prioritise effective responses and mitigations	
PPC-L3-SEC-107	PPCL2-SEC-001	**Security**	The Supplier shall produce and maintain incident response and recovery plans for all security incidents/breaches, including both identified and unidentified security Incidents/breaches; such plans to be reviewed and agreed by the Director on an annual basis.	
PPC-L3-SEC-108	PPCL2-SEC-001	**Security**	The Supplier shall test its own response and recovery plans and support testing of enterprise-wide response and recovery plans, at least on a quarterly basis, and after the implementation of significant change.	
PPC-L3-SEC-109	PPCL2-SEC-001	**Security**	The Supplier shall establish a baseline of network and system operations and expected data flows for the CIMS and provide this to the CSMS and the Director upon request.	
PPC-L3-SEC-110	PPCL2-SEC-001	**Security**	The Supplier shall assess the impact of events detected on the security of CIMS	
PPC-L3-SEC-111	PPCL2-SEC-001	**Security**	The Supplier shall monitor the physical environment to detect security incidents/breaches	
PPC-L3-SEC-112	PPCL2-SEC-001	**Security**	The Supplier shall monitor Personnel activity to detect security incidents/breaches	
PPC-L3-SEC-113	PPCL2-SEC-001	**Security**	The Supplier shall work with the CSMS to monitor external service providers activity for potential security incidents/breaches and communicate any detected incidents to the CSMS and the Director.	
PPC-L3-SEC-114	PPCL2-SEC-001	**Security**	The Supplier shall monitor for attempted connections to the CIMS by unauthorised personnel, devices, and software	
PPC-L3-SEC-115	PPCL2-SEC-001	**Security**	The Supplier shall define internal roles and responsibilities for detection and response to potential or confirmed security incidents/breaches, including nomination of a lead point of contact with the Director's security representatives and the CSMS	
PPC-L3-SEC-116	PPCL2-SEC-001	**Security**	The Supplier shall ensure that detection processes do not breach any other applicable requirements	
PPC-L3-SEC-117	PPCL2-SEC-001	**Security**	The Supplier shall test their own detection processes on a quarterly basis and share the results of such tests with the Director	
PPC-L3-SEC-118	PPCL2-SEC-001	**Security**	The Supplier shall communicate detected security incidents to the Director and the CSMS, in accordance with agreed criteria and timeliness	
PPC-L3-SEC-119	PPCL2-SEC-001	**Security**	In preparation for potential security incidents/breaches, the Supplier shall produce and agree with the Director Incident Response and Recovery Plans and Strategies for security incidents which pose greatest risk of breaching the tolerances in the Statement of Information Risk Appetite and ensure that Plans and Strategies are communicated to Responders and are updated in the light of lessons learned from any security incidents/breaches.	
PPC-L3-SEC-120	PPCL2-SEC-001	**Security**	The Supplier shall support the preparation of and execution of Incident Response and Recovery Plans at the Directors request even where the security incident/breach is not believed to have arisen on the CIMS, under the coordination of the CSMS.	
PPC-L3-SEC-121	PPCL2-SEC-001	**Security**	The Supplier shall ensure that Incident Response and Recovery plans identify roles and responsibilities and allocate these to named and suitably qualified individuals, whose details shall be shared with the Director and the CSMS. Where required by the Incident Response and Recovery plan, responders need to be available 24/7	
PPC-L3-SEC-122	PPCL2-SEC-001	**Security**	If the Supplier becomes aware of a potential or actual Security Incident/Breach it shall notify the Director and the CSMS in accordance with, and to timescales established within, the Security Incident Management Process as set out in the Security Management Plan.	
PPC-L3-SEC-123	PPCL2-SEC-001	**Security**	In the event of a suspected Breach of Security affecting the CIMS, the Supplier shall immediately communicate the details to the Director and other parties within the CIMS as directed by the Director; the Supplier shall provide such information on the matter as reasonably requested by those parties in order to address any risks posed by the Breach of Security	
PPC-L3-SEC-124	PPCL2-SEC-001	**Security**	The Supplier shall share information about threats and vulnerabilities with organisations agreed by the Director in order to achieve broader cybersecurity situational awareness	
PPC-L3-SEC-125	PPCL2-SEC-001	**Security**	Where Security Incidents or Breaches are suspected the Supplier shall immediately make available suitably skilled and experienced resource to engage in diagnosis/validation and response planning	
PPC-L3-SEC-126	PPCL2-SEC-001	**Security**	The Supplier shall initiate investigation of, and response to, suspected Security Incidents/Breaches within the CIMS (whether identified by the Supplier or the CSMS). The Supplier shall collaborate with the Director or the CSMS in the investigation of, and response to, suspected Security Incidents within the WIMS.	
PPC-L3-SEC-127	PPCL2-SEC-001	**Security**	The Supplier shall, as soon as reasonably practicable and, in any event, within 2 Working Days, following a Breach of Security or attempted Breach of Security, provide to the Director full details of the Breach of Security or attempted Breach of Security, including a root cause and impact analysis and shall subsequently update the Director on a daily basis any changes in the root cause and impact analysis until all mitigation activities are completed.	
PPC-L3-SEC-128	PPCL2-SEC-001	**Security**	The Supplier shall support any investigation of incidents/breaches for legal, disciplinary or other reasons, including where necessary using digital forensic analysis capabilities	
PPC-L3-SEC-129	PPCL2-SEC-001	**Security**	The Supplier shall validate all potential security incidents/breaches and assign a predefined category/severity upon which the appropriate incident/breach response can be initiated.	
PPC-L3-SEC-130	PPCL2-SEC-001	**Security**	The Supplier shall subscribe to authoritative sources of vulnerability information including CVSS and vulnerability alerts issued by providers of software within the CIMS and shall also receive vulnerability information received from these sources or by the Director from NCSC, or any other Central Government Body.	
PPC-L3-SEC-131	PPCL2-SEC-001	**Security**	The Supplier shall implement a mechanism for analysing and acting upon received vulnerability information	
PPC-L3-SEC-132	PPCL2-SEC-001	**Security**	Where a security incident/breach is suspected the Supplier shall immediately take all reasonable steps (which shall include any action or changes reasonably required by the Director) necessary to contain the Security Incident/Breach and minimise the damage and risk posed.	
PPC-L3-SEC-133	PPCL2-SEC-001	**Security**	Where the Supplier believes that there are residual risks associated with a vulnerability which are within the Director's appetite, the Supplier shall document the residual risk to the Director.	
PPC-L3-SEC-134	PPCL2-SEC-001	**Security**	In the event of a Security Incident/Breach the Supplier shall execute a planned procedure to restore all service critical systems or assets to normal running and capacity.	
PPC-L3-SEC-135	PPCL2-SEC-001	**Security**	The Supplier shall implement succession or continuity plans in the event of the loss of staff critical to cyber resilience	

PPC-L3-SEC-136	PPCL2-SEC-001	**Security**	After a Security Incident/Breach the Supplier shall conduct a documented lessons learned exercise, which shall include consideration of the root cause analysis. The Supplier shall mitigate the root cause and undertake improvements identified in the lessons learned analysis such as implementing additional security controls to remove such vulnerabilities or weaknesses from the CIMS. Security Incident/Breach plans will also be updated where necessary and within 2 weeks.	
PPC-L3-SEC-137	PPCL2-SEC-001	**Security**	After a Security Incident/Breach the Supplier shall update its recovery strategies to reflect lessons learnt from the recovery from the Security Incident/Breach.	
PPC-L3-SEC-138	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the Director is provided with the information the Director requires in order to issue appropriate statements to the media with regard to any security incident.	
PPC-L3-SEC-139	PPCL2-SEC-001	**Security**	After a Security Incident/Breach the Supplier shall communicate its recovery activities to the Director, the CSMS, and where required to the Suppliers of the WIMS.	
PPC-L3-SEC-140	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the Director is provided with the information the Director needs in order to ensure the Director can meet expectations of all stakeholders and ensure that incidents/breaches are reported in line with regulations imposed by external stakeholders.	
PPC-L3-SEC-141	PPCL2-SEC-001	**Security**	The Supplier must record incidents, breaches and near misses. Management processes with clearly allocated responsibilities must be in place to reflect and learn from incidents, breaches and near misses. All such records must be provided to the Director through monthly reporting and governance meetings.	
PPC-L3-SEC-142	PPCL2-SEC-001	**Security**	The Supplier shall take external security events, changing Threats, industry specific intelligence, changes in best practice and views from the into account whilst continually improving its Security Management Plan and control environment	
PPC-L3-SEC-143	PPCL2-SEC-001	**Security**	The Supplier shall undertake red team testing on at least an annual basis reporting the results to the Director and the CSMS and ensuring identified vulnerabilities/risks are mitigated in line with the requirements of Volume 3, Schedule 2.4 (Security).	
PPC-L3-SEC-144	PPCL2-SEC-001	**Security**	The Supplier shall undertake purple team testing in conjunction with the Director's CSMS (Central Security Monitoring Service) annually, reporting results to the Director and ensure that any identified issues/risks/threats/vulnerabilities are mitigated in line with the requirements of Volume 3, Schedule 2.4 (Security).	
PPC-L3-SEC-145	PPCL2-SEC-001	**Security**	The Supplier shall comply with the Director's Information Asset Management Framework.	
PPC-L3-SEC-146	PPCL2-SEC-001	**Security**	This requirement has been removed (duplicate of PPC-L3-SEC-002).	The Supplier shall comply with the current HMG Security Policy Framework.
PPC-L3-SEC-147	PPCL2-SEC-001	**Security**	This requirement has been removed (duplicate of PPC-L3-SEC-002)	The Supplier shall comply the HMG Security Classifications for Information Assets.
PPC-L3-SEC-148	PPCL2-SEC-001	**Security**	The Supplier shall comply with the Director's offshoring of information assets policy.	
PPC-L3-SEC-149	PPCL2-SEC-001	**Security**	The Supplier shall comply with the Director's data transfer procedures and the Director's data transmission policy.	
PPC-L3-SEC-150	PPCL2-SEC-001	**Security**	The Supplier shall ensure that the Director is compliant with the Public Records Act 1958 and shall report compliance to the Director on a monthly basis.	
PPC-L3-SEC-151	PPCL2-SEC-001	**Security**	Information assets shall be processed fairly, lawfully, and in a transparent manner.	
PPC-L3-SEC-152	PPCL2-SEC-001	**Security**	Information assets processed by the service shall be adequate, relevant, and limited to what is necessary in relation to the purpose for which it's processed.	
PPC-L3-SEC-153	PPCL2-SEC-001	**Security**	The solution shall identify all information assets, their sources, destinations and possible routes from source to destination.	
PPC-L3-SEC-154	PPCL2-SEC-001	**Security**	All information assets shall be maintained in an Information Asset Register which must be provided to the Director for assurance.	
PPC-L3-SEC-155	PPCL2-SEC-002	**Security**	The Supplier shall ensure that any connections to the WIMS (Wider Information Management System), where agreed by the Director, are secure, including mutual authentication and protection of data in transit.	
PPC-L3-SEC-156	PPCL2-SEC-002	**Security**	The Supplier shall ensure that any Director Data transmitted between its services are encrypted whilst in transit.	
PPC-L3-SEC-157	PPCL2-SEC-002	**Security**	The Supplier shall ensure that any Director Data transmitted between its services are encrypted if it comes to rest during the transmission process	
PPC-L3-SEC-158	PPCL2-SEC-002	**Security**	The Supplier shall ensure that encrypted data can only be decrypted by systems administrators within a controlled procedure	
PPC-L3-SEC-159	PPCL2-SEC-002	**Security**	The Supplier shall provide authentication credentials to the Integration Platform using the protocols and processes defined by the Integration Platform Supplier	
PPC-L3-SEC-160	PPCL2-SEC-002	**Security**	The Supplier shall be able to securely authenticate the Integration Platform when connecting services, using recognised industry standards for strong authentication as defined by the Integration Platform Supplier	
PPC-L3-SEC-161	PPCL2-SEC-002	**Security**	The Supplier shall enforce service re-authentication of the Integration Platform at time periods agreed with the Director	
PPC-L3-SEC-162	PPCL2-SEC-002	**Security**	The Supplier shall comply with the policies, processes, guidelines and standards for the secure use of the Integration Platform, as defined by the Integration Platform Supplier.	
PPC-L3-SEC-163	PPCL2-SEC-002	**Security**	The Supplier shall manage any dependencies to allow secure use of the services by the Director and its Suppliers	
PPC-L3-SEC-164	PPCL2-SEC-002	**Security**	The Supplier shall implement, and only implement external connections that have been agreed by the Director through an Enterprise Architecture process	
PPC-L3-SEC-165	PPCL2-SEC-002	**Security**	The Supplier shall meet the Director's security vetting requirements as identified in Schedule 2.4.	
PPC-L3-SEC-166	PPCL2-SEC-002	**Security**	The Supplier shall ensure the integrity and non-reputability of messages transmitted by its services, so that the recipient of a message can trust the veracity of its sender and content.	
PPC-L3-SEC-167	PPCL2-SEC-002	**Security**	The Supplier solution shall be aligned with the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance and (where software-as-a-service is used to deliver components of the service) the NCSC SaaS Security Principles and accompanying guidance	The Supplier solution shall be compliant with the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance and (where software-as-a-service is used to deliver components of the service) the NCSC SaaS Security Principles and accompanying guidance.
PPC-L3-SEC-168	PPCL2-SEC-002	**Security**	The Supplier shall maintain alignment with the current versions of the NCSC Cloud Security Principles and NCSC SaaS Security Principles throughout the life of the contract.	The Supplier shall maintain compliance with the current versions of the NCSC Cloud Security Principles and NCSC SaaS Security Principles throughout the life of the contract.
PPC-L3-SEC-169	PPCL2-SEC-002	**Security**	The Supplier solution shall be compliant with the current HMG Minimum Cyber Security Standards.	
PPC-L3-SEC-170	PPCL2-SEC-002	**Security**	The Supplier shall maintain compliance with the current version of the HMG Minimum Cyber Security Standards (or equivalent provisions that are defined to replace them) throughout the life of the contract.	
PPC-L3-SEC-171	PPCL2-SEC-002	**Security**	The Supplier shall ensure that Solution is securely implemented in accordance with good industry practice and shall validate this through testing and supply evidence to the Director through the security reporting process.	The Supplier shall ensure that Solution is securely implemented so that it is not susceptible to the OWASP Top 10 Web Application Security Risks, in accordance with good industry practice and shall validate this through testing and supply evidence to the Director through the security reporting process.
PPC-L3-SEC-172	PPCL2-SEC-002	**Security**	The Supplier shall ensure that Solution is not susceptible to the latest version of the OWASP Top 10 Web Application Security Risks, throughout the life of the contract and shall validate this through testing and supply evidence to the Director through the security reporting process.	
PPC-L3-SEC-173	PPCL2-SEC-002	**Security**	The Supplier shall ensure that, where relevant, Solution is compliant with the current Payment Card Industry Data Security Standard (PCI-DSS) and shall ensure that compliance is maintained throughout the life of the contract, validated through testing and evidenced to the Director through the security reporting process.	
PPC-L3-SEC-174	PPCL2-SEC-002	**Security**	The Supplier shall ensure that any service(s) or application(s) are designed to be Secure by Default, in line with the relevant NCSC guidance, and shall provide evidence to the Director through monthly governance forum	
PPC-L3-SEC-175	PPCL2-SEC-002	**Security**	The Supplier shall protect any emails sent on the behalf of the organisation in transit, in line with relevant NCSC guidance. At a minimum, this should include the use of the minimum acceptable version of TLS as recommended by NCSC.	
PPC-L3-SEC-176	PPCL2-SEC-002	**Security**	The Supplier shall treat email and SMS as insecure media and not send any sensitive information (to be agreed with the Director, but including any information that could be used by an attacker to facilitate further identity attacks) over all channels.	
PPC-L3-SEC-177	PPCL2-SEC-002	**Security**	The Supplier shall ensure that all communications of sensitive information (as identified in response to requirement N-012) with customers shall be conducted using secure messaging systems that require authentication to access and that protect data in transit using approved cryptographic methods.	
PPC-L3-SEC-178	PPCL2-SEC-002	**Security**	The Supplier shall ensure that multi-factor authentication is used for all access to social media accounts that represent the Director, and that usage aligns with current NCSC guidance	
PPC-L3-SEC-179	PPCL2-SEC-002	**Security**	The Supplier shall ensure that only authorised staff are able to access social media accounts that represent the Director, as required.	
PPC-L3-SEC-180	PPCL2-SEC-002	**Security**	The Supplier shall ensure that control of all social media accounts relating to the service is handed over to the Director on termination of the contract.	
PPC-L3-SEC-181	PPCL2-SEC-002	**Security**	The Supplier shall ensure the customer has been appropriately authenticated (including the use of Strong Customer Authentication where applicable) in accordance with the Directors risk tolerance and good security practice, so that only identified and authorised customers are able to interact with banking and other services.	The Supplier shall ensure the customer has been appropriately authenticated (including the use of Strong Customer Authentication where applicable) in accordance with the Directors risk tolerance and good security practice, so that only identified and authorised customers are able to interact with banking and other services The Supplier shall ensure the customer has been appropriately authenticated in accordance with the Directors risk tolerance and good security practice.
PPC-L3-SEC-182	PPCL2-SEC-003	**Security**	The Supplier shall ensure that additional authentication can be applied to a customer action, where required (whether identified by the Supplier or where indicated by another Supplier within the WIMS).	
PPC-L3-SEC-183	PPCL2-SEC-003	**Security**	The Supplier shall ensure that where multiple alternative methods of authentication are available to customers to access their accounts, they do not increase the overall risk to the Director or the customer, so that the Director's risk profile remains consistent across channels.	The Supplier shall ensure that where multiple alternative methods of authentication are available to customers to access their accounts, they do not increase the overall risk to the Director or the customer.
PPC-L3-SEC-184	PPCL2-SEC-003	**Security**	Where applicable, any authentication, authorisation and federation protocols must use open standards and be interoperable, extensible and vendor-agnostic, so that the Director can integrate with other suppliers' authentication solutions and benefit from new technologies.	Where applicable, any authentication, authorisation and federation protocols must use open standards and be vendor-agnostic.

PPC-L3-SEC-185	PPCL2-SEC-003	**Security**	The Supplier shall test, evaluate and audit the strong customer authentication processes and the security measures in place to protect the customer credentials on a monthly basis and provide evidence to the Director through the security reporting process.	The Supplier shall test, evaluate and audit the strong customer authentication processes and the security measures in place to protect the customer credentials on a monthly basis and provide evidence to the Director through the security reporting process.
PPC-L3-SEC-186	PPCL2-SEC-003	**Security**	This requirement has been removed	The supplier shall provide a capability to enable voice biometric authentication
PPC-L3-SEC-187	PPCL2-SEC-003	**Security**	The Supplier shall make use of the authentication service provided by the Digital Experience and Digital Enablement Supplier to authenticate customers, where applicable, so that there is a robust authentication process, single sign-on and joined up audit trail of customer activity.	The supplier shall make use of the federated authentication service provided by each supplier, where applicable, to authenticate staff or support users, so that there is a single sign on and a joined up audit trail of user activity The Supplier shall make use of the federated authentication service, provided by Other Suppliers, where applicable
PPC-L3-SEC-188	PPCL2-SEC-003	**Security**	The Supplier shall ensure that customer accounts may be accessed and managed securely by designated proxies.	
PPC-L3-SEC-189	PPCL2-SEC-003	**Security**	The Supplier shall ensure that all proxy access is audited and accountable, and that authentication processes are as strong as with regular access.	
PPC-L3-SEC-190	PPCL2-SEC-003	**Security**	The Supplier shall conduct and share with the Director a documented risk assessment process, consistent with the Director's risk management framework, to consider the impact on customer experience and ease-of-use of implementing security controls.	
PPC-L3-SEC-191	PPCL2-SEC-003	**Security**	The Director and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to identify where additional access management controls are required. Roles which are likely to require additional access management controls include: - Provider Personnel with Enhanced Privileges (root, system administrator, database administrator or equivalent); - Provider Personnel with access to live Bulk Customer Data or copies of the live Bulk Customer Data; - Provider Personnel working in an information security role or with responsibility for managing information security personnel; - Provider Personnel working in a financial crime role where those individuals have access to details relating to criminal investigations or with responsibility for managing financial crime personnel; and - Provider Personnel roles with non-administrative/privileged access to Bulk Customer Data where: *access is to full copies of live Bulk Customer Data that allows individuals to be identified; *access is not being controlled by the application to single records only; and *no audit trail of access to information records is created.	
PPC-L3-SEC-192	PPCL2-SEC-003	**Security**	Where additional access management is required, the Supplier shall ensure that Staff access the system using multifactor authentication.	
PPC-L3-SEC-193	PPCL2-SEC-003	**Security**	The Supplier shall ensure that all resources used for enhanced privilege access (root, system administrator, database administrator or equivalent) are dedicated to this privileged access and not used for any other purpose.	
PPC-L3-SEC-194	PPCL2-SEC-003	**Security**	The Supplier shall apply the 'principle of least privilege' when allowing privileged access to the Supplier System, including the use of time-limited authorisation where appropriate.	
PPC-L3-SEC-195	PPCL2-SEC-004	**Security**	The Supplier shall ensure that all physical and logical interfaces for any application(s), and means of accessing data, are fully documented and evidenced to the Director.	
PPC-L3-SEC-196	PPCL2-SEC-004	**Security**	The Supplier shall ensure that mutual strong authentication is enabled for all communications with external services; the strength of authentication shall be agreed with the Director.	
PPC-L3-SEC-197	PPCL2-SEC-004	**Security**	The Supplier shall ensure that all information exchanged with external services is protected in transit using approved cryptographic means.	
PPC-L3-SEC-198	PPCL2-SEC-004	**Security**	The Supplier shall federate identity and access management provision with the Integration Platform as required, using industry standards protocols as specified by the Integration Platform provider.	
PPC-L3-SEC-199	PPCL2-SEC-004	**Security**	The Supplier shall federate identity and access management provision with other Suppliers within the WIMS as required, using industry standards protocols as specified by the Integration Platform provider.	
PPC-L3-SEC-200	PPCL2-SEC-004	**Security**	The Supplier shall ensure that all assisted digital activities undertaken by the contact centre are fully logged and audited.	
PPC-L3-SEC-201	PPCL2-SEC-004	**Security**	The solution for assisted digital access by the contact centre shall not require the customer to download or install additional software.	
PPC-L3-SEC-202	PPCL2-SEC-004	**Security**	The Supplier shall ensure that any assisted digital solution that allows access by contact centre staff shall redact any sensitive information that is not required by the contact centre operator (to be agreed with the Director, but including credentials and debit card details for example).	
PPC-L3-SEC-203	PPCL2-SEC-004	**Security**	The solution shall provide controls to ensure separation of duties according to defined criteria, for activities undertaken by Supplier staff or by staff from other Suppliers in the WIMS, as required by the Director.	
PPC-L3-SEC-204	PPCL2-SEC-004	**Security**	The Supplier shall provide an Identity Provider (IdP) capability for Supplier Staff that can federate with multiple other supplier solutions within the WIMS, using protocols specified by the Director.	The Supplier shall provide an Identity Provider (IdP) capability for Supplier Staff that can federate with other supplier solutions within the WIMS, using protocols specified by the Director.
PPC-L3-SEC-205	PPCL2-SEC-004	**Security**	The Supplier's federated IdP capability shall include attributes for each individual, as required and specified by the Director.	
PPC-L3-SEC-206	PPCL2-SEC-004	**Security**	The Supplier shall implement processes to ensure that the IdP attributes are correct for each individual, and remain correct throughout the lifetime of the system.	
PPC-L3-SEC-207	PPCL2-SEC-004	**Security**	The Supplier shall provide an access management capability that can federate with multiple other supplier solutions within the WIMS, using protocols specified by the Director.	The Supplier shall provide an access management capability that can federate with other supplier solutions within the WIMS, using protocols specified by the Director.
PPC-L3-SEC-208	PPCL2-SEC-004	**Security**	The Supplier's federated access management capability shall ensure that access is only provided to authenticated individuals, as required by the Directors identity and access management (IDAM) model.	
PPC-L3-SEC-209	PPCL2-SEC-004	**Security**	The Supplier's federated access management capability shall ensure that access is only provided to authorised individuals as required by, and using the attributes identified within, the Directors identity and access management (IDAM) model.	
PPC-L3-SEC-210	PPCL2-SEC-005	**Security**	The Supplier shall provide a means for internal service users to report security vulnerabilities or issues, and shall use this feedback to inform future development of any services or application(s)	
PPC-L3-SEC-211	PPCL2-SEC-005	**Security**	The Supplier shall conduct proactive threat intelligence activities in order to identify new and emerging threats relating to their Services.	
PPC-L3-SEC-212	PPCL2-SEC-005	**Security**	The Supplier shall conduct market research relating to financial customer security trends.	
PPC-L3-SEC-213	PPCL2-SEC-005	**Security**	The Supplier shall, on a quarterly basis, review the security measures in place, in accordance with sector threats and market research, and make proposals for improvements, where required, to ensure best-practice security implementation.	
PPC-L3-SEC-214	PPCL2-SEC-005	**Security**	The Supplier shall implement measures to counter use of fake emails purporting to come from the organisation's domains, in line with relevant NCSC guidance. At a minimum, this should include the use of the most recent versions of DMARC, SPF and DKIM.	
PPC-L3-SEC-215	PPCL2-SEC-005	**Security**	The Supplier shall forward on any suspicious email communications received to a reporting service identified by the Director, that will investigate and remove scam email addresses and websites.	
PPC-L3-SEC-216	PPCL2-SEC-005	**Security**	The Supplier shall implement measures to enable customers to verify that they are interacting with an authorised service representing the Director.	
PPC-L3-SEC-217	PPCL2-SEC-005	**Security**	The Supplier shall implement best practice measures when corresponding or interacting with customers to help them to differentiate authorised communications from fraudulent communications, such as (but not limited to) not putting links in text messages sent to customers.	The Supplier shall implement best practice measures when corresponding with customers to help them to differentiate authorised communications from fraudulent communications, such as (but not limited to) not putting links in text messages sent to customers.
PPC-L3-SEC-218	PPCL2-SEC-006	**Security**	The Supplier shall identify, plan and design the collection and transmission of log and event data to the central security monitoring service (CSMS), in accordance with the CSMS requirements.	
PPC-L3-SEC-219	PPCL2-SEC-006	**Security**	The Supplier shall ensure that communications undertaken with the Director or other parties in conjunction with incident detection, response and recovery are undertaken using consistent reporting formats supplied by the CSMS.	
PPC-L3-SEC-220	PPCL2-SEC-006	**Security**	The Supplier shall provide log and event data to the CSMS to enable it monitor the CIMS.	
PPC-L3-SEC-221	PPCL2-SEC-006	**Security**	The Supplier shall collaborate with the CSMS to establish alerting criteria to indicate anomalous or suspicious behaviour	
PPC-L3-SEC-222	PPCL2-SEC-006	**Security**	The Supplier shall immediately inform the Director and the CSMS where a security incident is identified and undertake remediating activities. The Supplier will be responsible for keeping the Director and the CSMS informed throughout the incident response and recovery activities.	
PPC-L3-SEC-223	PPCL2-SEC-006	**Security**	The Supplier shall fulfil all Roles and Responsibilities as defined by the CSMS to ensure there is a clear approach to the detection and response to cyber security incidents, including those spanning multiple Supplier infrastructures (cross-provider attacks).	
PPC-L3-SEC-224	PPCL2-SEC-006	**Security**	The Supplier shall develop, implement and test response plans (every six months) to ensure that they are able to respond to cyber security incidents, and shall support and liaise with the CSMS to enable coordination and response to cyber security incidents that span multiple Supplier infrastructures.	
PPC-L3-SEC-225	PPCL2-SEC-006	**Security**	Where required, the Supplier shall support the CSMS in investigating, co-ordinating and responding to potential cross-Supplier attacks.	
PPC-L3-SEC-226	PPCL2-SEC-006	**Security**	In the event of either a suspected or confirmed attack, the Supplier shall respond to the incident and liaise with the CSMS, and (in the event of a cross-Supplier attack) with other Suppliers across the WIMS.	

PPC-L3-SEC-227	PPCL2-SEC-006	**Security**	The Supplier shall implement appropriate countermeasures as a consequence of Threat Intelligence provided by the Director as part of their status as an HMG organisation.	
PPC-L3-SEC-228	PPCL2-SEC-006	**Security**	The Supplier shall assess, prioritise, communicate and receive Threat Intelligence from the CSMS and shall implement appropriate countermeasures as a consequence, communicating these to the Director.	
PPC-L3-SEC-229	PPCL2-SEC-006	**Security**	The Supplier shall identify, document and communicate cyber security threats/risks/vulnerabilities, both internal and external, based on Threat Intelligence to the CSMS and the Director.	
PPC-L3-SEC-230	PPCL2-SEC-006	**Security**	The Supplier shall work with the CSMS to implement further countermeasures to identify and target indicators of compromise which could lead to cross-party attacks	
PPC-L3-SEC-231	PPCL2-SEC-006	**Security**	The Supplier shall establish and maintain Incident Response and Recovery Playbooks/Plans and co-operate with the CSMS for scenarios which cover potential or actual cross-Supplier attacks.	
PPC-L3-SEC-232	PPCL2-SEC-006	**Security**	The Supplier shall establish and maintain Incident Response and Recovery Playbooks/Plans and co-operate with the CSMS and the Director in the event of suspicion of a potential indicator of compromise which is yet to be validated.	
PPC-L3-SEC-233	PPCL2-SEC-006	**Security**	The Supplier shall conduct rehearsal and testing of Response and Recovery Playbook/Plans and shall coordinate with the CSMS in the rehearsal and testing of cross-Supplier attacks so that the ability of the organisation to respond to Key Scenarios is suitably assured.	
PPC-L3-SEC-234	PPCL2-SEC-006	**Security**	The Supplier shall, subject to agreement with the Director, implement further incident response preparatory measures, so that the response can make full use of the Supplier's capabilities.	
PPC-L3-SEC-235	PPCL2-SEC-006	**Security**	The Supplier shall comply with audit and logging requirements defined by the CSMS so that cross-party attacks and potential security incidents can be identified and responded to appropriately.	
PPC-L3-SEC-236	PPCL2-SEC-006	**Security**	The Supplier shall ensure that all assets (including all devices, applications, infrastructure, networks, hardware, software, tooling and systems) used to provide services to the Director as part of the CIMS, where prescribed by the Director, are appropriately monitored as directed by the CSMS so that incidents are identified, reported and acted upon.	The Supplier shall ensure that all devices, applications, infrastructure, networks, hardware, software, tooling and systems used to provide services to the Director are appropriately monitored as directed by the CSMS so that incidents are identified, reported and acted upon. This will include all subcontractors deployed by the Supplier.
PPC-L3-SEC-237	PPCL2-SEC-006	**Security**	The Supplier shall act on alerts provided by the CSMS, which could relate to either a potential or actual cross-party attack affecting the services provided to the Director or a potential or actual attack which is limited to the Supplier.	
PPC-L3-SEC-238	PPCL2-SEC-006	**Security**	The Supplier shall define the criteria for initialising the Security Impact Assessment process.	
PPC-L3-SEC-239	PPCL2-SEC-006	**Security**	Where an attack is suspected, the Supplier shall provide a rapid security impact assessment so that the validity of the alert is ascertained and an appropriate response can be initiated.	
PPC-L3-SEC-240	PPCL2-SEC-006	**Security**	The Supplier shall co-operate with the CSMS with investigations initiated following any attacks on the Supplier or wider cross-party attacks on the WIMS, so that the root causes can be established and lessons learned can be incorporated into cyber security defences.	
PPC-L3-SEC-241	PPCL2-SEC-006	**Security**	The Supplier shall conduct threat hunting and communicate the results to the CSMS and the Director, where potential or actual indicators of compromise are identified in the CIMS.	
PPC-L3-SEC-242	PPCL2-SEC-006	**Security**	The Supplier shall maintain and periodically review key scenarios at least every 6 months.	
PPC-L3-SEC-243	PPCL2-SEC-006	**Security**	The Supplier shall provide an initial Security Impact Assessment (Validation) of suspected: - P1 security incident within 15 minutes - P2 security incident within 60 minutes - P3 security incident within 240 minutes	
PPC-L3-SEC-244	PPCL2-SEC-006	**Security**	The Supplier shall report P1 security incidents to the Director and the CSMS within 30 minutes of the conclusion of the Security Impact Assessment.	
PPC-L3-SEC-245	PPCL2-SEC-006	**Security**	The Supplier shall report P2 security incidents to the Director and the CSMS within 90 minutes of the conclusion of the Security Impact Assessment.	
PPC-L3-SEC-246	PPCL2-SEC-006	**Security**	The Supplier shall manage the completion of the activities documented in incident response and recovery playbooks/plans within agreed timescales for 98% of incidents	
PPC-L3-SEC-247	PPCL2-SEC-006	**Security**	When recommended by the CSMS, the Supplier shall take steps to mitigate threats/risk highlighted during threat intelligence review.	
PPC-L3-SEC-248	PPCL2-SEC-006	**Security**	The Supplier shall highlight Threat Intelligence indicating increased external risk to the Director and the CSMS within one day of its receipt	
PPC-L3-SEC-249	PPCL2-SEC-006	**Security**	The Supplier shall participate in testing to validate the effectiveness of the cyber capabilities and defences deployed on at least an annual basis.	
PPC-L3-SEC-250	PPCL2-SEC-006	**Security**	The Supplier shall work with the CSMS to ensure that all devices, and external service providers where relevant, within the scope of the CIMS are monitored by the Central Security Monitoring service. This collaborative activity will be completed monthly.	
PPC-L3-SEC-251	PPCL2-SEC-006	**Security**	The Supplier shall assist the CSMS in defining a security baseline for normal processes and user behaviour so that anomalies are easier to identify.	
PPC-L3-SEC-252	PPCL2-SEC-006	**Security**	The Supplier shall comply with the specification of co-operation required by monitored parties, as provided by the CSMS.	
PPC-L3-SEC-253	PPCL2-SEC-006	**Security**	The Supplier shall provide all relevant data required to allow the CSMS to effectively monitor the Director's IT estate.	
PPC-L3-SEC-254	PPCL2-SEC-006	**Security**	The Supplier shall follow the architectural and implementation patterns for the collection and transfer of data provided by the Director and/or its CSMS. This activity will be reviewed by the Director's enterprise architecture forum and security personnel.	
PPC-L3-SEC-255	PPCL2-SEC-006	**Security**	The Supplier shall collaborate with the CSMS to agree the scope and approach for the collection of data. This will be reviewed by the Director.	
PPC-L3-SEC-256	PPCL2-SEC-006	**Security**	The Supplier shall collaborate with the CSMS to tune and continually improve the monitoring results of its systems. Changes shall be reported to the Director through governance processes.	
PPC-L3-SEC-257	PPCL2-SEC-006	**Security**	The Supplier shall comply with the policy, processes, standards and guidelines for the provision of data to the CSMS, and shall review such compliance quarterly, or when the documents are updated.	
PPC-L3-SEC-258	PPCL2-SEC-006	**Security**	The Supplier shall undertake training provided by the CSMS Supplier, and co-operate as required, to ensure a collaborative approach to the protective monitoring of the Director's business.	
PPC-L3-SEC-259	PPCL2-SEC-007	**Security**	The Supplier shall ensure that any service(s) or application(s) are designed to be Secure by Default, in line with NCSC guidance.	
PPC-L3-SEC-260	PPCL2-SEC-007	**Security**	The Supplier shall define, implement and operate secure software development and deployment systems and environments in accordance with the NIST Secure Software Development Framework (SSDF) and other relevant industry best practice, agreed with the Director. The Supplier shall provide ongoing evidence for assurance review to the Director through the security reporting process.	The Supplier shall define, implement and operate secure software development and deployment systems in accordance with the NIST Secure Software Development Framework (SSDF). The Supplier shall provide ongoing evidence for assurance review to the Director through the security reporting process.
PPC-L3-SEC-261	PPCL2-SEC-008	**Security**	The Supplier shall maintain a record at all times of compliance with key security requirements, as determined by the Director, and shall provide evidence to the Director through security governance processes on a monthly basis as a minimum, and on request.	
PPC-L3-SEC-262	PPCL2-SEC-008	**Security**	The Supplier shall undertake a continual controls assurance process to verify the ongoing efficacy of the implemented security controls, and shall provide evidence to the Director through security governance processes on a monthly basis as a minimum, and on request.	
PPC-L3-SEC-263	PPCL2-SEC-008	**Security**	The Supplier shall provide regular information to the Director, to include patching, vulnerability management, security testing, change management, compliance management, logging and monitoring, incident planning and exercising, incident response and recovery, risks and issues, on a monthly basis as a minimum, and on request.	
PPC-L3-SEC-264	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall develop, implement and continually improve the business continuity procedures and plans in accordance with Industry Best Practice.	
PPC-L3-SEC-265	PPCL2-SEC-009	**Security**	The Supplier shall comply with the Director's Business Continuity Policy.	
PPC-L3-SEC-266	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall create policy documents covering business continuity and review these against the Director's Policies. Any gaps and areas of non-compliance will be agreed with the Director and rectified prior to the Service Commencement Date.	
PPC-L3-SEC-267	PPCL2-SEC-009	**Security**	The Supplier shall develop a Business Continuity Strategy in compliance with the Directors Business Continuity Policy, which covers the services provided and is agreed with the Director 12 weeks prior to service commencement date	
PPC-L3-SEC-268	PPCL2-SEC-009	**Security**	The Supplier shall propose Recovery Time Objectives (RTO's) aligned to their strategy, such RTO's must be agreed by the Director 12 weeks prior to service commencement date.	
PPC-L3-SEC-269	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall design and implement a business continuity management system (BCMS) certified to ISO22301 covering the scope agreed and accepted by the Director.	
PPC-L3-SEC-270	PPCL2-SEC-009	**Security**	The Supplier shall fully comply with the BCI Good Practice Guidelines by ensuring that the areas addressed by the BCI Guidelines are covered by its approach to BCP. The key areas covered by the guidelines are: a) Policy and Programme Management b) Embedding c) Analysis d) Design e) Implementation f) Validation	

PPC-L3-SEC-271	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall implement a business continuity management (BCM) strategy that will maintain Services to the Director in compliance with agreed recovery time objectives by identifying key risks and threats to the continuity of the business and by deploying appropriate mitigating measures and strategies.	
PPC-L3-SEC-272	PPCL2-SEC-009	**Security**	The Supplier's BCM strategy shall be fully integrated with relevant Subcontractors' Business Continuity Plans. The resilience of Services and the required recovery targets for Subcontractors will be specified and included in contractual terms and service level agreements, aligned to the Director's BIA and recovery objectives.	
PPC-L3-SEC-273	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Supplier shall ensure that any changes to the Services or Service Delivery Solution (including Changes to organisational functions, processes and systems) will not weaken the business continuity management arrangements unless the Director expressly agrees otherwise.	
PPC-L3-SEC-274	PPCL2-SEC-009	**Security**	The Suppliers shall undertake a Business Impact Analysis ("BIA"), to identify risk, threats and vulnerabilities that may lead to potential loss of, or disruption to, the Services. This is a documented deliverable to the Director for review.	
PPC-L3-SEC-275	PPCL2-SEC-009	**Security**	The Supplier shall complete the BIA and submit a report setting out its findings (the "BIA Report") for the Director's review no later than 12 weeks prior to the Service Commencement Date.	
PPC-L3-SEC-276	PPCL2-SEC-009	**Security**	The Supplier shall undertake a BIA annually, on each anniversary of the Service Commencement Date, or additionally as may be determined by the Director, acting reasonably, and, following the implementation of any Changes to the Services, or the Provider's Service Delivery Solution.	
PPC-L3-SEC-277	PPCL2-SEC-009	**Security**	The Supplier shall undertake a BIA annually, on each anniversary of the Service Commencement Date, or additionally as may be determined by the Director, acting reasonably, and, following the implementation of any Changes to the Services, or the Provider's Service Delivery Solution.	
PPC-L3-SEC-278	PPCL2-SEC-009	**Security**	Each BIA Report shall be a Documentary Deliverable and shall be subject to Director review.	
PPC-L3-SEC-279	PPCL2-SEC-009	**Security**	The Supplier shall incorporate any changes to the draft BIA Report that the Director may request and shall re-submit a revised draft of the BIA Report.	
PPC-L3-SEC-280	PPCL2-SEC-009	**Security**	The Supplier shall produce and maintain plans (the "Business Continuity Plans") which shall incorporate all elements of each BIA.	
PPC-L3-SEC-281	PPCL2-SEC-009	**Security**	The Business Continuity Plans shall be submitted to the Director within 20 Working Days of the Director's review of the BIA Report.	
PPC-L3-SEC-282	PPCL2-SEC-009	**Security**	The Business Continuity Plans shall set out the timescales for each element of the Services to be fully recovered for each Service element, including business functions, systems and processes on the occurrence of a Business Continuity Event (the "Recovery Time Objectives").	
PPC-L3-SEC-283	PPCL2-SEC-009	**Security**	The Supplier shall ensure that the Recovery Time Objectives do not exceed the Maximum Tolerable Period of Disruption or Maximum Acceptable Outage.	
PPC-L3-SEC-284	PPCL2-SEC-009	**Security**	The Supplier shall ensure that on the occurrence of a Business Continuity Event all Services are available within the timescales set out in the Recovery Time Objectives.	
PPC-L3-SEC-285	PPCL2-SEC-009	**Security**	The Business Continuity Plans shall clearly set out those Services which the supplier will relocate/recover on the occurrence of a Business Continuity Event, the proposed recovery location/strategy and the timescales for relocation. The Supplier shall not relocate Services to any location other than a location which been acknowledged by the Director in advance	
PPC-L3-SEC-286	PPCL2-SEC-009	**Security**	The Supplier shall ensure that the Business Continuity Plans as minimum: *are up to date and cover all aspects of the Services *align with any supporting Operational Incident management procedures and documentation and include cross references to such documentation; *are updated to take account of any Changes including any resulting from each BIA; and *include a communications strategy that shall be implemented on the occurrence of a Business Continuity Event.	
PPC-L3-SEC-287	PPCL2-SEC-009	**Security**	The Business Continuity Plans shall be available for review by the Director immediately upon the Director's request	
PPC-L3-SEC-288	PPCL2-SEC-009	**Security**	Changes to Business Continuity Plans shall be subject to the review by the Director	
PPC-L3-SEC-289	PPCL2-SEC-009	**Security**	In the event of any invocation of the Business Continuity Plans the Supplier shall keep the Director fully informed as the Director requires	
PPC-L3-SEC-290	PPCL2-SEC-009	**Security**	All communications required, during the occurrence of a Business Continuity Event until Services are fully recovered, shall be agreed with the Director prior to any such communications.	
PPC-L3-SEC-291	PPCL2-SEC-009	**Security**	The Supplier shall notify the Director of all Business Continuity Events immediately. Where the supplier cannot notify the Director immediately, it shall, notify the Director within four (4) hours.	
PPC-L3-SEC-292	PPCL2-SEC-009	**Security**	On the occurrence of one (1) or more Business Continuity Events which, either separately or cumulatively, mean that the Services, or a material part of the Services, will be unavailable for a period of time which has a critical impact on the Services, the Supplier shall notify the Director within one (1) hour of such Business Continuity Event(s).	
PPC-L3-SEC-293	PPCL2-SEC-009	**Security**	The Supplier shall undertake a regular programme of exercises and tests in accordance with Industry Best Practice and shall set out in a report, to be delivered to the Director, the duration, scope, aims, programme and frequency of the BC Exercises and Tests. The frequency of Tests shall be agreed with the Director and will occur at least on a biannual basis. The BC Exercises and Tests programme shall be updated as part of the BIA and reviewed bi-monthly with the Director	
PPC-L3-SEC-294	PPCL2-SEC-009	**Security**	The Supplier shall ensure that BC Exercises and Tests shall not have any impact on the live environment or impact live services.	
PPC-L3-SEC-295	PPCL2-SEC-009	**Security**	The Director shall have the right to be fully involved with the BC Exercises and Tests.	
PPC-L3-SEC-296	PPCL2-SEC-009	**Security**	Within four weeks of completion of any BC Exercises and Tests, the supplier shall provide the Director with a report setting out as a minimum: the details and outcome of the BC Exercises and Tests; any failures, identified in the Business Continuity Plans and systems, including lessons learnt and a root cause analysis; the proposals and specific actions, including a timetable for implementation, for remedying any failures and process improvements. The Supplier shall amend the Business Continuity Plans where the BC Exercises and Tests identify any gaps in the resilience and availability needs of the Services	
PPC-L3-SEC-297	PPCL2-SEC-009	**Security**	The Supplier shall provide a formal training, awareness and educational learning programme on Business Continuity appropriate to individuals' roles in Business Continuity arrangements, for all supplier Personnel. This programme shall include refresher training following each Business Impact Assessment or any material change to the Business Continuity Plans	
PPC-L3-SEC-298	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	In the event of another of the Directors suppliers invoking a business continuity incident for its own service, the supplier shall provide support to ensure the ongoing availability of the Director's end-to-end service	
PPC-L3-SEC-299	PPCL2-SEC-009	**Security (Business Continuity/ Disaster Recovery)**	The Director has the right to audit the supplier's business continuity management arrangements on an annual basis, the timing of which will be determined by the Director	
PPCL3-SIM-001	PPCL2-SIM-001	**SIAM**	The Supplier shall assist SIAM in the creation of the end to end component and application overview to enable the development and ongoing maintenance of the Availability Plan	
PPCL3-SIM-002	PPCL2-SIM-001	**SIAM**	The Supplier shall review and approve the Availability Plan provided by SIAM	
PPCL3-SIM-003	PPCL2-SIM-001	**SIAM**	The Supplier shall evaluate the effectiveness of its own availability management process and implement changes to its availability management process to improve efficiency	
PPCL3-SIM-004	PPCL2-SIM-001	**SIAM**	The Supplier shall work with SIAM and other Suppliers to assist with any other Suppliers engagement as agreed in the collaboration agreement	
PPCL3-SIM-005	PPCL2-SIM-001	**SIAM**	The Supplier shall provide SIAM with a detailed impact for new/amended availability requirements	
PPCL3-SIM-006	PPCL2-SIM-002	**SIAM**	The Supplier shall provide application/service availability data to SIAM to enable the measurement of end-to-end availability of the services	
PPCL3-SIM-007	PPCL2-SIM-002	**SIAM**	The Supplier shall provide the required data feeds to SIAM for the measurement of the defined Director's critical business transactions	
PPCL3-SIM-008	PPCL2-SIM-002	**SIAM**	The Supplier shall undertake Component Failure Impact Analysis (CFIA) and Single Points of Failure (SPOF) analysis and make the results available to the Director's SIAM function	
PPCL3-SIM-009	PPCL2-SIM-002	**SIAM**	The Supplier shall ensure that appropriate levels of monitoring of resources and system performance are set and that information recorded is kept up to date	
PPCL3-SIM-010	PPCL2-SIM-002	**SIAM**	The Supplier shall support any ad-hoc audits that are carried out on the capacity management process as per Part 3 para 1.2	
PPCL3-SIM-011	PPCL2-SIM-002	**SIAM**	The Supplier shall provide a data feed to SIAM on used and available capacity	
PPCL3-SIM-012	PPCL2-SIM-002	**SIAM**	The Supplier shall analyse the business forecasts and provide their periodical capacity plan in the required format to SIAM	
PPCL3-SIM-013	PPCL2-SIM-002	**SIAM**	The Supplier shall ensure that forecast narratives and data are realistic, consistent and align with the Director's business forecasts, IS/IT Strategies and reflect known Project engagement	
PPCL3-SIM-014	PPCL2-SIM-002	**SIAM**	The Supplier shall ensure the capacity plan demonstrates an understanding between business demand, use of IT related services and resource unit consumption	
PPCL3-SIM-016	PPCL2-SIM-002	**SIAM**	The Supplier shall respond to and resolve any queries raised in relation to the capacity plan	
PPCL3-SIM-017	PPCL2-SIM-002	**SIAM**	The Supplier shall, where required, undertake further analysis of the identified optimisation opportunity and produce a plan that incorporates the analysis and benefits and prioritises other Suppliers activity and discuss with SIAM/the Director as appropriate	

PPCL3-SIM-018	PPCL2-SIM-002	**SIAM**	The Supplier shall, when approved, produce a plan for implementation of the proposed optimisation opportunity and manage the activities within the plan through to a successful conclusion, reporting progress and any issues to SIAM as they occur	
PPCL3-SIM-019	PPCL2-SIM-002	**SIAM**	The Supplier shall, where required, provide information to SIAM to support the optimisation opportunity analysis	
PPCL3-SIM-021	PPCL2-SIM-002	**SIAM**	The Supplier shall comply with any reasonable request by the SIAM function to provide relevant data in the required formats and frequency to enable the SIAM function to provide and manage the end to end capacity management process	
PPCL3-SIM-022	PPCL2-SIM-002	**SIAM**	The Supplier shall provide an effective impact assessment process for analysing service capacity requirements as a result of a business change provided by the Director	
PPCL3-SIM-023	PPCL2-SIM-002	**SIAM**	The Supplier shall ensure that the forecast narrative provides sufficient information to enable the Director to understand the risks and consequences associated with any action/inaction, the timescales until problems will be experienced and recommended mitigation action to eliminate or minimise impacts, the likely costs associated with remedial options/action and the decisions required by the Director	
PPCL3-SIM-024	PPCL2-SIM-002	**SIAM**	The Supplier shall provide insight into performance achieved focusing on exceptional performance, performance that does not meet expectations and any underlying issues and actions required to resolve those issues	
PPCL3-SIM-025	PPCL2-SIM-002	**SIAM**	The Supplier shall monitor, analyse and report to SIAM on capacity volumes and trends	
PPCL3-SIM-026	PPCL2-SIM-002	**SIAM**	The Supplier shall manage capacity related changes through to a successful conclusion and confirm they have had the required effect on the management of capacity	
PPCL3-SIM-027	PPCL2-SIM-003	**SIAM**	The Supplier shall escalate to SIAM any cross-Service Provider issues that cannot be resolved directly between the other Suppliers	
PPCL3-SIM-028	PPCL2-SIM-003	**SIAM**	The Supplier shall work with SIAM and other Suppliers to assist with any Service Provider engagement and non-compliance issues	
PPCL3-SIM-029	PPCL2-SIM-003	**SIAM**	The Supplier shall provide all necessary details and information of such Service Impacting Event	
PPCL3-SIM-030	PPCL2-SIM-003	**SIAM**	The Supplier shall investigate, contain, track, manage, resolve and report events before any service impact occurs	
PPCL3-SIM-031	PPCL2-SIM-004	**SIAM**	The Supplier shall conduct IT Service Continuity awareness activities within the Service Provider IT Service Continuity team	
PPCL3-SIM-032	PPCL2-SIM-004	**SIAM**	The Supplier shall perform Service Threat assessments as directed by the Director's SIAM and / or Risk functions and inform SIAM of the outcome	
PPCL3-SIM-033	PPCL2-SIM-004	**SIAM**	The Supplier shall analyse root cause analysis and incident closure reports and inform SIAM of the outcome and raise any current and emerging ITSCM risks required	
PPCL3-SIM-034	PPCL2-SIM-004	**SIAM**	The Supplier shall produce the Service Provider IT Service Continuity Plan and agree it with SIAM	
PPCL3-SIM-035	PPCL2-SIM-004	**SIAM**	The Supplier shall analyse new projects or project changes to determine whether sufficient information is provided in order to enable impact assessment to be undertaken	
PPCL3-SIM-036	PPCL2-SIM-004	**SIAM (Disaster Recovery)**	The Supplier shall identify any project or change related IT Service Continuity risks and emerging risks and take appropriate action to mitigate those risks	
PPCL3-SIM-037	PPCL2-SIM-004	**SIAM**	The Supplier shall produce and update IT Service Continuity products including Test Recovery Plans, disaster recovery plans and business continuity plans, as appropriate	
PPCL3-SIM-038	PPCL2-SIM-004	**SIAM**	The Supplier shall provide information to SIAM to assist in the completion of the IT Service Continuity Test Programme	
PPCL3-SIM-039	PPCL2-SIM-004	**SIAM**	The Supplier shall contribute to the high level IT Service Continuity Test Plan and produce its own low level test plans	
PPCL3-SIM-040	PPCL2-SIM-004	**SIAM**	The Supplier shall analyse the test results of test activity and provide input to the test report and the action plan for any remedial activities	
PPCL3-SIM-041	PPCL2-SIM-004	**SIAM (Disaster Recovery)**	The Supplier shall complete any actions required as detailed in the action plan	
PPCL3-SIM-042	PPCL2-SIM-004	**SIAM**	The Supplier shall participate in the execution of a ITSCM Test Plan, Disaster Recovery Plans and Business Continuity Plans and the real ITSCM event as needed with the relevant Director functions and Other Suppliers	
PPCL3-SIM-043	PPCL2-SIM-005	**SIAM**	The Supplier shall work with SIAM and the Director as reasonably required with the scoping of audits, impact assessments, investigation and resolution of discrepancies	
PPCL3-SIM-045	PPCL2-SIM-005	**SIAM**	The Supplier shall review and comment on audit scope documents	
PPCL3-SIM-046	PPCL2-SIM-005	**SIAM**	The Supplier shall monitor, analyse and report to SIAM on the accuracy of the other Suppliers configuration management database and provide evidence of proactive configuration management to SIAM at the service asset and configuration management service review meetings	
PPCL3-SIM-047	PPCL2-SIM-005	**SIAM**	The Supplier shall monitor, analyse and report to SIAM on the accuracy of the other Suppliers configuration management database and provide evidence of proactive configuration management to SIAM at the service asset and configuration management service review meetings	
PPCL3-SIM-048	PPCL2-SIM-005	**SIAM**	The Supplier shall provide agreed configuration management measurements to SIAM	
PPCL3-SIM-049	PPCL2-SIM-005	**SIAM**	The Supplier shall develop changes to their interfaces and continuous improvement data content as defined in the interface definition documentation provided by SIAM	
PPCL3-SIM-050	PPCL2-SIM-005	**SIAM**	The Supplier shall test changes to their interfaces and continuous improvement data content as defined in the interface definition documentation provided by SIAM	
PPCL3-SIM-051	PPCL2-SIM-005	**SIAM**	The Supplier shall implement changes to their interfaces and CI data content as defined in the interface definition documentation provided by SIAM	
PPCL3-SIM-052	PPCL2-SIM-005	**SIAM**	The Supplier shall provide CI data in accordance with the interface requirements of the integrated CMDB	
PPCL3-SIM-053	PPCL2-SIM-005	**SIAM**	The Supplier shall ensure that CI updates are processed in accordance with the SIAM Change Management Policies and Procedures	
PPCL3-SIM-054	PPCL2-SIM-006	**SIAM**	The Supplier shall provide the required audit data to SIAM within the required timescales and in the format specified	
PPCL3-SIM-055	PPCL2-SIM-006	**SIAM**	The Supplier shall develop a process (preferably automated or non-automated) for the provision of configuration data to SIAM	
PPCL3-SIM-057	PPCL2-SIM-007	**SIAM**	The Supplier shall provide SIAM with required asset attributes	
PPCL3-SIM-058	PPCL2-SIM-007	**SIAM**	The Supplier shall raise requests in the appropriate format to request service provider changes to the service catalogue	
PPCL3-SIM-059	PPCL2-SIM-007	**SIAM**	The Supplier shall provide timely impact assessments to SIAM for any change requests raised by other Suppliers, SIAM and the Director	
PPCL3-SIM-060	PPCL2-SIM-007	**SIAM**	The Supplier shall provide management information for each Service Measurement Period to SIAM in accordance with the Service Level Management Policies and Procedures	
PPCL3-SIM-061	PPCL2-SIM-038	**SIAM**	The Supplier shall monitor and analyse Service Level/KPI performance and provide evidence and trend analysis to SIAM within agreed Service Management Period	
PPCL3-SIM-062	PPCL2-SIM-007	**SIAM**	The Supplier shall provide input to periodic service level management audit reviews when required	
PPCL3-SIM-063	PPCL2-SIM-008	**SIAM**	The Supplier shall provide dashboard information to SIAM as agreed	
PPCL3-SIM-064	PPCL2-SIM-009	**SIAM**	The Supplier shall undertake checks to ensure performance data provided to SIAM is accurate and complete	
PPCL3-SIM-065	PPCL2-SIM-009	**SIAM**	The Supplier shall address and resolve any queries with the service measurement period reports raised by the SIAM	
PPCL3-SIM-066	PPCL2-SIM-009	**SIAM**	The Supplier shall provide Impact Assessment for changes to SIAM policies and Procedures and documentation at SIAM's request	
PPCL3-SIM-067	PPCL2-SIM-009	**SIAM**	The Supplier shall raise invoices (including service credits) and associated supporting management information for products and service provided in accordance with the Service Provider contract terms and conditions	
PPCL3-SIM-068	PPCL2-SIM-009	**SIAM**	The Supplier shall provide SIAM with a feed of information relating to consumption of chargeable resources, catalogue requests and other change requests to enable service charges to be validated	
PPCL3-SIM-069	PPCL2-SIM-009	**SIAM**	The Supplier shall provide SIAM with a feed of performance, capacity, and availability data to enable verification that SLAs and KPIs have been met	
PPCL3-SIM-070	PPCL2-SIM-010	**SIAM**	The Supplier shall engage with SIAM to resolve invoice discrepancies	
PPCL3-SIM-071	PPCL2-SIM-010	**SIAM**	The Supplier shall refund incorrect payments as soon as possible	
PPCL3-SIM-072	PPCL2-SIM-010	**SIAM**	The Supplier shall work with SIAM and other Suppliers to assist with any engagement and non-compliance issues	
PPCL3-SIM-073	PPCL2-SIM-010	**SIAM**	The Supplier shall discuss with SIAM operational leads which service management processes are applicable to the Service Provider based on their contractual obligations	
PPCL3-SIM-074	PPCL2-SIM-010	**SIAM**	The Supplier shall identify any gaps in compliance with SIAM's policies and procedures and agree a plan to achieve compliance	
PPCL3-SIM-075	PPCL2-SIM-010	**SIAM**	The Supplier shall meet regularly with SIAM throughout the take-on progress to review progress towards compliancy	
PPCL3-SIM-076	PPCL2-SIM-011	**SIAM**	The Supplier shall agree sign-off that on-boarding has been complete	
PPCL3-SIM-077	PPCL2-SIM-012	**SIAM**	The Supplier shall work with SIAM and the Director as reasonably requested with the scoping of Exit Management Plan audits, impact assessments, investigation and resolution of discrepancies	
PPCL3-SIM-078	PPCL2-SIM-012	**SIAM**	The Supplier shall provide the required Exit Management audit data to SIAM within the required timescales and in the format specified	
PPCL3-SIM-079	PPCL2-SIM-012	**SIAM**	The Supplier shall provide named individuals to act as points of contact with SIAM	
PPCL3-SIM-080	PPCL2-SIM-013	**SIAM**	The Supplier shall provide information of Case Bases and Knowledge Articles to SIAM to update the Service Desk scripts	
PPCL3-SIM-081	PPCL2-SIM-013	**SIAM**	The Supplier shall regularly review and update Case Bases and Workarounds to ensure the currency of information contained in them and provide such information to the Service Desk	

PPCL3-SIM-082	PPCL2-SIM-013	**SIAM**	The Supplier shall provide details of the other Suppliers' support organisation and contacts points to SIAM to enable the accurate assignment of incidents by the Service Desk	
PPCL3-SIM-083	PPCL2-SIM-013	**SIAM**	The Supplier shall integrate with the SIAM Service monitoring/management tool(s) to facilitate automated assignment and update of incident data	
PPCL3-SIM-084	PPCL2-SIM-013	**SIAM**	The Supplier shall inform the Service monitoring/management tool(s) when they become aware of a fault or failure and indicate the impact to the Director	
PPCL3-SIM-085	PPCL2-SIM-013	**SIAM**	The Supplier shall accept and acknowledge incidents that are correctly assigned by the Service Desk	
PPCL3-SIM-086	PPCL2-SIM-013	**SIAM**	The Supplier shall return incorrectly assigned incidents to the Service Desk	
PPCL3-SIM-087	PPCL2-SIM-013	**SIAM**	The Supplier shall log all IT related incidents on the SIAM Integrated tool	
PPCL3-SIM-088	PPCL2-SIM-013	**SIAM**	The Supplier shall allocate incident severities in accordance with the Incident Severity definitions contained in the Incident Management Policies and Procedures	
PPCL3-SIM-089	PPCL2-SIM-013	**SIAM**	The Supplier shall provide updates to the SIAM function on the progress of incidents when requested to do so in accordance with the timescales defined in relation to incident severity	
PPCL3-SIM-090	PPCL2-SIM-014	**SIAM**	The Supplier shall inform the Service desk when an incident has been resolved and provide a valid resolution code by performing incident diagnosis on all incidents assigned to the service provider	
PPCL3-SIM-091	PPCL2-SIM-014	**SIAM**	The Supplier shall provide a feed of event and incident data to SIAM as required to enable detection of incidents affecting the Director customer services	
PPCL3-SIM-092	PPCL2-SIM-014	**SIAM**	The Supplier shall provide details of the other Suppliers support organisation and contacts points to SIAM	
PPCL3-SIM-093	PPCL2-SIM-014	**SIAM**	The Supplier shall accept and acknowledge service requests that are correctly assigned by the service desk	
PPCL3-SIM-094	PPCL2-SIM-014	**SIAM**	The Supplier shall return incorrectly assigned service requests to the service desk	
PPCL3-SIM-095	PPCL2-SIM-015	**SIAM**	The Supplier shall provide updates on the progress of service requests when requested to do so by the service desk	
PPCL3-SIM-096	PPCL2-SIM-015	**SIAM**	The Supplier shall inform the service desk when a service request has been completed	
PPCL3-SIM-097	PPCL2-SIM-015	**SIAM**	The Supplier shall provide management information each service management period to the appropriate service request forums in accordance with the service request management policies and procedures	
PPCL3-SIM-098	PPCL2-SIM-015	**SIAM**	The Supplier shall identify potential problems and raise with SIAM	
PPCL3-SIM-099	PPCL2-SIM-015	**SIAM**	The Supplier shall submit fully documented and validated problem records to SIAM using an agreed format and mechanism	
PPCL3-SIM-100	PPCL2-SIM-015	**SIAM**	The Supplier shall classify problems using SIAM's problem severity model	
PPCL3-SIM-101	PPCL2-SIM-015	**SIAM**	The Supplier shall log and track problems during their lifecycle	
PPCL3-SIM-102	PPCL2-SIM-015	**SIAM**	The Supplier shall accept and resolve problems when they are correctly assigned to the service provider	
PPCL3-SIM-103	PPCL2-SIM-016	**SIAM**	The Supplier shall provide progress updates on problems in a timely manner to SIAM	
PPCL3-SIM-104	PPCL2-SIM-017	**SIAM**	The Supplier shall perform root cause analysis on problems including developing corrective actions and/or workarounds / maintain known error logs for all problems	
PPCL3-SIM-105	PPCL2-SIM-017	**SIAM**	The Supplier shall continually evaluate the linked incident count to known errors and problems	
PPCL3-SIM-106	PPCL2-SIM-018	**SIAM**	The Supplier shall inform SIAM where it suspects inappropriate user access has been granted e.g. where the Service Provider suspects inappropriate access is granted during its investigation of an incident	
PPCL3-SIM-107	PPCL2-SIM-018	**SIAM**	The Supplier shall ensure that all relevant service information is made available to the Director's SIAM function so that the development of the service knowledge management repository is comprehensive	
PPCL3-SIM-108	PPCL2-SIM-018	**SIAM**	The Supplier shall ensure that all relevant service information is updated and made available when changes to the operational services mean that previously provided information is out of date and no longer reflects the operational services	
PPCL3-SIM-109	PPCL2-SIM-018	**SIAM**	The Supplier shall provide input to periodic Service Level Management audit reviews when required (ref Schedule 7.5)	
PPCL3-SIM-110	PPCL2-SIM-018	**SIAM**	The Supplier shall assist SIAM and the Director in the definition of the service levels, service targets and KPIs	
PPCL3-SIM-111	PPCL2-SIM-019	**SIAM**	The Supplier shall fully define new or amended service levels, and KPI requirements	
PPCL3-SIM-112	PPCL2-SIM-019	**SIAM**	The Supplier shall confirm the service level management impact arising from new or amended service levels, service targets and KPI requirements and submit to the SIAM for approval	
PPCL3-SIM-113	PPCL2-SIM-020	**SIAM**	The Supplier shall propose a timetable for the implementation and activation of new/amended service levels, service targets and KPIs	
PPCL3-SIM-114	PPCL2-SIM-020	**SIAM**	The Supplier shall attend service provider compliance management meetings where required by SIAM	
PPCL3-SIM-115	PPCL2-SIM-020	**SIAM**	The Supplier shall put in place and manage remedial action plans to resolve non-compliance	
PPCL3-SIM-116	PPCL2-SIM-020	**SIAM**	The Supplier shall review and approve the plan to deliver service transition	
PPCL3-SIM-117	PPCL2-SIM-021	**SIAM**	The Supplier shall complete all activities in the service transition delivery plan that are assigned to the Service Provider	
PPCL3-SIM-118	PPCL2-SIM-021	**SIAM**	The Supplier shall proactively contribute to cost saving opportunities	
PPCL3-SIM-119	PPCL2-SIM-021	**SIAM**	The Supplier shall provide transformation delivery & cost optimisation plans	
PPCL3-SIM-120	PPCL2-SIM-021	**SIAM**	The Supplier shall log and track changes during their lifecycle ensuring that SIAM has visibility of changes throughout the lifecycle	
PPCL3-SIM-121	PPCL2-SIM-021	**SIAM**	The Supplier shall ensure that Change Proposal submitted comprehensively in a timely manner	
PPCL3-SIM-122	PPCL2-SIM-021	**SIAM**	The Supplier shall ensure that any Requests for Change raised has sufficient justification and are submitted in sufficient time to avoid the need for SIAM to initiate urgent action to ensure the change is implemented to the required timescale.	
PPCL3-SIM-123	PPCL2-SIM-021	**SIAM**	The Supplier shall ensure the Requests for Change record is updated during its lifecycle and contains the accurate CAB score prior to be issued for impact assessment	
PPCL3-SIM-124	PPCL2-SIM-021	**SIAM**	The Supplier shall ensure that any cancelled Requests for Change identify the reasons for the cancellation	
PPCL3-SIM-125	PPCL2-SIM-021	**SIAM**	The Supplier shall ensure that evaluations of impact are returned within the required timescale and that the correct information is included to aid the progression of the change request	
PPCL3-SIM-126	PPCL2-SIM-022	**SIAM**	The Supplier shall ensure that change deployment will be planned to minimise disruption to operational services	
PPCL3-SIM-127	PPCL2-SIM-022	**SIAM**	The Supplier shall ensure that changes raised are scheduled during a scheduled maintenance window or other time approved by SIAM	
PPCL3-SIM-128	PPCL2-SIM-022	**SIAM**	The Supplier shall ensure the change owner brokers positive impact assessment and endeavours to resolve negative impacts	
PPCL3-SIM-129	PPCL2-SIM-022	**SIAM**	The Supplier shall provide draft implementation plans to SIAM as set out in schedule 6.1	
PPCL3-SIM-130	PPCL2-SIM-023	**SIAM**	The Supplier shall perform allocated service provider activities on the consolidated implementation plans	
PPCL3-SIM-131	PPCL2-SIM-023	**SIAM**	The Supplier shall attend and contribute to the implementation walkthrough	
PPCL3-SIM-132	PPCL2-SIM-024	**SIAM**	The Supplier shall provide product catalogue, release plans and roadmaps to SIAM package releases in accordance with the release management strategy	
PPCL3-SIM-133	PPCL2-SIM-024	**SIAM**	The Supplier shall provide early life support immediately after deployment of a change	
PPCL3-SIM-134	PPCL2-SIM-024	**SIAM**	The Supplier shall provide a mechanism for automatically rolling back IT changes to restore operations to a known state in the event of problems introduced or revealed by a change	
PPCL3-SIM-135	PPCL2-SIM-024	**SIAM**	The Supplier shall review the project documentation appropriate to OAT (Operational Acceptance Testing) and SMAT (Service Management Acceptance Testing) and provide comments to SIAM	
PPCL3-SIM-136	PPCL2-SIM-024	**SIAM**	The Supplier shall provide OAT and SMAT strategies and plans to SIAM for review	
PPCL3-SIM-137	PPCL2-SIM-024	**SIAM**	The Supplier shall perform allocated service provider activities on the consolidated OAT and SMAT plans	
PPCL3-SIM-138	PPCL2-SIM-024	**SIAM**	The Supplier shall provide service provider OAT and SMAT test completion reports to SIAM and review and sign-off the consolidated OAT and SMAT test completion reports	
PPCL3-SIM-139	PPCL2-SIM-029	**SIAM**	The Supplier shall review transition requirements and contribute to the transition approach	
PPCL3-SIM-140	PPCL2-SIM-025	**SIAM**	The Supplier shall provide assurance about service provider deliverables and transition activity to SIAM prior to the operational readiness review	
PPCL3-SIM-141	PPCL2-SIM-025	**SIAM**	The Supplier shall participate as required by changes being made by SIAM and other managed other Suppliers	
PPCL3-SIM-142	PPCL2-SIM-026	**SIAM**	The Supplier shall participate in testing activities required by changes being made by other Suppliers	
PPCL3-SIM-143	PPCL2-SIM-026	**SIAM**	The Supplier shall provide future project activity Information so that the Director's SIAM function can assess and schedule future test environment availability	
PPCL3-SIM-144	PPCL2-SIM-026	**SIAM**	The Supplier shall upskill the Director's IT Ops Senior Leadership Team to the extent that the team is comfortable to start Agile/DevOps discussions and drive the DevOps Change agenda.	
PPCL3-SIM-145	PPCL2-SIM-026	**SIAM**	The Supplier shall communicate with all Suppliers any changes which may impact on the objectives, behaviours and outcomes of the support model to minimise any impact on services and people	
PPCL3-SIM-146	PPCL2-SIM-026	**SIAM**	The Supplier shall implement Relationship Management processes so that appropriate interfaces between other Suppliers and SIAM to ensure the protection of End-to End service delivery	

PPCL3-SIM-147	PPCL2-SIM-026	**SIAM**	The Supplier shall provide capability for receiving knowledge and insights as required by Director to ensure that the appropriate information, data and knowledge is provided	
PPCL3-SIM-148	PPCL2-SIM-026	**SIAM**	The Supplier shall ensure that there is an operations capability to contain, share, save knowledge (not limited to processes etc) so that the business is able to function effectively	
PPCL3-SIM-149	PPCL2-SIM-022	**SIAM**	The Supplier shall provide provisions for the management of the transfer of internal and external staff to deliver end-to-end services in the new operating model to ensure smooth transition of all staff including clarity of roles and responsibilities.	
PPCL3-WOW-001	PPCL2-SIM-028	**SIAM**	The Supplier shall identify opportunities for optimising capacity in capacity plans and recommend appropriate action	
PPCL3-WOW-002	PPCL2-SIM-035	**SIAM**	The Supplier shall provide the required audit data to SIAM within the required timescales and in the format specified by SIAM	
PPCL3-WOW-003	PPCL2-SIM-037	**SIAM**	The Supplier shall provide advance notice of changes the Supplier plans to make and have an opportunity to agree or amend the change schedule.	
PPCL3-WOW-004	PPCL2-SIM-028	**SIAM**	The Supplier shall liaise with the Director's SIAM function and other service provider project management functions so that full coverage of service delivery is ensured	
PPCL3-WOW-005	PPCL2-SIM-028	**SIAM**	The Supplier shall integrate and contribute to Director mandated knowledge management and collaboration tooling so that a central repository of corporate information is maintained	
PPCL3-WOW-006	PPCL2-SIM-028	**SIAM**	The Supplier shall align with the cross-Supplier collaborative ways of working so that the Director and its Suppliers can work efficiently to achieve their common aims	
PPCL3-WOW-007	PPCL2-SIM-028	**SIAM**	The Supplier shall support the Director in delivering insight-driven continuous improvement and delivery so that the Director can improve services frequently, iteratively and cost-effectively	
PPCL3-WOW-008	PPCL2-SIM-027	**SIAM**	The Supplier shall ensure delivery and continuous improvements are driven by actionable insight into business drivers, customer needs and behaviours, and operational performance so that the Director reduces the risk and maximises the effectiveness of change	
PPCL3-WOW-009	PPCL2-SIM-036	**SIAM**	The Supplier shall operate with appropriate levels of devolved authority so that teams are self-sufficient and empowered to act on insight and can prioritise their deliverables	
PPCL3-WOW-010	PPCL2-SIM-030	**SIAM**	The Supplier shall communicate with the Director and its Suppliers, sharing knowledge openly and transparently so that teams are empowered and have the information they need to make decisions	
PPCL3-WOW-011	PPCL2-SIM-031	**SIAM**	The Supplier shall align with the Director's change governance so that the accountabilities and responsibilities for change and its risks, are clearly defined, understood, and managed	
PPCL3-WOW-012	PPCL2-SIM-032	**SIAM**	The Supplier shall align with the Director's cadence of delivery so that management and delivery of change is coordinated across Suppliers, release paths, and touchpoints	
PPCL3-WOW-013	PPCL2-SIM-032	**SIAM**	The Supplier shall leverage customer, competitor and market intelligence so that the Director can maintain its fast follower status, ensuring it refreshes its capabilities in line with emerging hygiene factors and best practice in digital services	
PPCL3-WOW-014	PPCL2-SIM-032	**SIAM**	The Supplier shall provide access to resources appropriately skilled in: •Service design; •UX design; •CX design; •UI design; •Accessibility and inclusive design; •Content design; •Visual design; •Application of brand and content guidelines; •Front-end development; •Widget and component development; •Customer testing; •Functional testing; •Configuration of the digital banking experience platform; •Copy writing and editing; •Analytics and critical thinking to provide insights, •Business analysis; •Technical architecture; •Agile working and scrum management; so that the Director can develop and deliver digital services to meet customers' needs and expectations	
PPCL3-WOW-015	PPCL2-SIM-032	**SIAM**	The Supplier shall provide a flexible, scalable, robust, and future-proof customer testing methodology, including as appropriate: •Customer research; •Testing of prototypes with appropriate fidelity; •Customer panel testing; •Split testing (A/B MVT testing, experimentation) ; so that the Director can be assured that services are comprehensively tested by customers before launch.	
PPCL3-WOW-016	PPCL2-SIM-032	**SIAM**	The Supplier shall provide a dedicated resource pool which can support DevOps Change activities (DevOp Change activities include: continuous improvement, projects and transformations, unforeseen changes, optimisation. This is further defined in Volume 3, Schedule 8.2 - Change Control Procedure), so that there is a distinction to the teams running the Service (IT Ops) versus those deployed to DevOps Change.	
PPCL3-WOW-017	PPCL2-SIM-033	**SIAM**	The Supplier shall implement and undertake DevOps activities to support delivery of Change (defined in Volume 3, Schedule 8.2 - Change Control Procedure). Activities included, but are not limited to: defining DevOps ambitions (to-be analysis), defining principles and standards for DevOps, defining, piloting and refining the DevOps model(s) to be adopted and defining DevOps measurements (KPI's).	
PPCL3-WOW-018	PPCL2-SIM-035	**SIAM**	The Supplier shall support DevOps Change of all sizes - both incremental and large-scale changes - through the provision of Agile Dev/Ops resources.	
PPCL3-WOW-019	PPCL2-SIM-034	**SIAM**	The Supplier shall provide a dedicated resource pool to deliver DevOps Change activities across all Digital Touchpoints delivered by the Supplier.	
PPCL3-WOW-020	PPCL2-SIM-032	**SIAM**	The Supplier shall provide a dedicated DevOps Change resource pool which operates in accordance with the Director's agreed Performance Indicators.	
PPCL3-WOW-021	PPCL2-SIM-032	**SIAM**	The Supplier shall build and manage the DevOps Change backlog on a sprint by sprint basis, ensuring deliverables meet stakeholder requirements and highest priority actions are executed, whilst the Director maintains ultimate ownership of the backlog.	
PPCL3-WOW-022	PPCL2-SIM-027	**SIAM**	The Supplier shall facilitate the transfer of knowledge between the dedicated DevOps Change resource pool and Director staff.	
PPCL3-TRF-001	PPCL2-TRF-001	**Transformation**	The Supplier shall define a comprehensive Customer Digital Migration strategy for the Director's approval. The strategy will enable the Supplier to achieve customer migration to digital of transformational scale, whilst ensuring agility, responsiveness and flexibility to changing customer and market needs, working in collaboration with the Director and other Suppliers. So that the Director can achieve the strategic aims of the Rainbow programme.	The Supplier shall provide a proposal as to how they will assist in developing a comprehensive strategy to achieve customer migration to digital of transformational scale, which ensures agility, responsiveness and flexibility to changing customer and market needs whilst working in collaboration with the Director and other Suppliers.
PPCL3-TRF-002	PPCL2-TRF-001	**Transformation**	The Supplier will regularly engage in dialogue with the Director and other Suppliers to review and adjust the approach to execution of the Customer Migration to Digital programme.	The Supplier shall provide a strategy as to how they anticipate the Director will best achieve comprehensive Customer digital migration strategy, taking into account the role of Other Suppliers and he Director.
PPCL3-TRF-003	PPCL2-TRF-001	**Transformation**	The supplier strategy shall include the methods and activities proposed to support a higher take up rate in self-service by customers, while maintaining service continuity and a positive experience for all customers so that the Director can be assured of a successful migration and on-going customer satisfaction during the migration.	The Supplier will propose a strategy as to how they will directly influence customers to adopt the digital route whilst operating within the boundaries of their specific functional responsibilities.
PPCL3-TRF-004	PPCL2-TRF-001	**Transformation**	In defining the strategy, the supplier shall provide an approach to ensure a strong influence from customers, considering their differing needs, preferences, vulnerabilities and motivations of customers, so that the director can provide an inclusive service and a service that is tailored to the customers' and Director's needs.	The Supplier shall provide an approach to ensure a strong influence from customers on the outcomes and improvements of the digital experience across all Supplier services to meet customer needs and experiences so that customer feedback is fed into the improvements adopted
PPCL3-TRF-005	PPCL2-TRF-001	**Transformation**	The supplier shall demonstrate how the success of the strategy will be measured, including but not limited to; metrics for customer migration to digital services and measures of customers' experience of the migration, so that Director can be assured that the strategy is not being positively received by customers and is on track to deliver its desired outcomes.	The Supplier shall provide an approach to track success in migrating customers to self-service and proposed metrics, to monitor take up rate of self-service by customers whilst monitoring that high quality and timely customer experience is maintained.
PPCL3-AD-177	PPCL2-AD-001	**Assisted Digital**	The Supplier shall provide Agent supported services from 8:00 a.m. till 8:00 p.m. Monday to Friday, and 8:00 a.m. to 6:00 p.m. on Saturdays and Sundays (Closed on Bank Holidays), and shall have the flexibility to change so that the director can meet any future business needs	
PPCL3-AD-178	PPCL2-AD-018	**Assisted Digital**	The supplier shall provide its contact centre agents with information, provided by the Director's other suppliers, on where a customer is on their digital self service journey, so that the contact centre agents are able to assist customers to complete their 'Jobs to be Done'	
PPCL3-AD-179	PPCL2-AD-018	**Assisted Digital**	The supplier shall ensure that contact centre agents are familiar with the customer's view of the digital self-service channels (including functionality and 'look and feel'), across all supported devices and browsers, so that the contact centre agents are able to assist customers to complete their 'Jobs to be Done' regardless of the method used by a customer.	

PPCL3-AD-180	PPCL2-AD-003	**Assisted Digital**	The supplier must provide the capability for agents to undertake and complete Jobs to be done on behalf of the customers through assisted digital channels, so that the Director can be assured that the supplier is able to resolve cases that customers are unable to complete.	
PPCL3-AD-181	PPCL2-AD-003	**Assisted Digital**	The supplier shall ensure it keeps pace with the developments and enhancements of the self-serve services that are provided by the Directors other suppliers, so that the agents are continuously able to assist customers through assisted digital channels by completing their jobs to be done	
PPCL3-AD-182	PPCL2-AD-003	**Assisted Digital**	The supplier shall provide a system that that allows for cases to be routed automatically directed to the correct agent, based on factors such as skillset and availability, so that customers are appropriately dealt with.	
PPCL3-AD-183	PPCL2-AD-003	**Assisted Digital**	The supplier shall design and implement workflows to assist customers in completing their journeys, that are consistent with, but not necessarily identical to self service journeys, so that the customer experience is similar across self service and assisted journeys.	
PPCL3-AD-184	PPCL2-AD-003	**Assisted Digital**	The supplier shall work with the integration platform provider and other service providers, to define the strategic interfaces needed to complete agent tasks (which may require reading and updating customer information and instructing banking transactions), so that the Directors other suppliers can expose services needed to complete agent facing journeys.	
PPCL3-AD-185	PPCL2-AD-003	**Assisted Digital**	The supplier shall ensure that that the Directors customer engagement history is updated with any interactions and actions taken, as a result of assisting customers with their jobs to done, so that the Director has an accurate record of customer history.	
PPCL3-AD-186	PPCL2-AD-003	**Assisted Digital**	The supplier shall provide appropriate and efficient tools for customer service agents including any required productivity tools, analytics and customers views, so that the Director can be assured the supplier is able to appropriately and efficiently assist the customer	
PPCL3-AD-187	PPCL2-AD-003	**Assisted Digital**	The supplier shall ensure that agents are able to access the right information when required, including accessing information held by other Director service suppliers, when dealing with customer queries, so that resolutions can be quickly resolved at first attempt.	
PPCL3-AD-188	PPCL2-AD-003	**Assisted Digital**	The supplier shall provide a means of assisting the agent to communicate with the customer where suitable and frequent customer requests are presented, to ensure a consistency of experience for the customers.	
PPCL3-AD-189	PPCL2-AD-003	**Assisted Digital**	The supplier shall provide service analytics, giving the Director easy access to reporting data, including not limited to backlog analysis, chatbot performance, case history and volume, agent productivity and activity, so that the director can manage performance and appropriately act.	
PPCL3-AD-190	PPCL2-AD-003	**Assisted Digital**	The supplier shall provide service analytics, giving the Director easy access to reporting data, including not limited to backlog analysis, chatbot performance, case history and volume, agent productivity and activity, so that the director can manage performance and appropriately act.	
PPCL3-AD-191	PPCL2-AD-015	**Assisted Digital**	The Suppliers messaging solution shall include the ability to use virtual agents to handle to common interactions with the customer, so that customers can have their queries answered immediately at any time.	
PPCL3-AD-192	PPCL2-AD-008	**Assisted Digital**	The Supplier shall ensure that customers can receive a transcript of their chats, so that the customer can hold a complete view of their interactions.	
PPCL3-ART-193	PPCL2-ART-009	**Architecture**	The Supplier shall collaborate with the Director and Other Suppliers to support change initiatives (including but not limited providing advisory, delivery and insight on potential approaches), so that change is delivered efficiently and effectively	
PPCL3-ART-194	PPCL2-ART-009	**Architecture**	The Supplier shall continuously facilitate knowledge transfer of change delivery methodologies to the Directors teams, so that the Directors capabilities are appropriately upskilled	
PPCL3-ART-195	PPCL2-ART-009	**Architecture**	The Supplier shall undertake, and engage with the Director and other suppliers, in regular, periodic planning at the strategic and portfolio level, as set out by the Director, so that strategic plans and roadmaps are aligned at all levels and change is delivered efficiently and effectively	
PPC-L3-SEC-300	PPCL2-SEC-003	**Security**	The Supplier shall ensure that the use of all Cloud Services within their Solution complies with the Directors Cloud Security Standard, so that Director can be assured that the solution meets the Director's Risk Appetite.	The Suppliers Customer authentication solution shall be standards-based, interoperable and extensible, so that the Director can integrate with other suppliers' authentication solutions and benefit from new technologies
PPCL3-AD-193	PPCL2-AD-007	**Assisted Digital**	The supplier shall ensure that, where feasible, customers accessing services through the telephony channel are authenticated and identified before they are connected to an agent so that the agent can be assured that they are talking with the customer or their authorised representative.	
PPC-L3-SEC-301	PPCL2-SEC-003	**Security**	The Supplier shall ensure that any new regulatory requirements relating to customers or their proxies accessing online banking services (including but not limited to Strong Customer Authentication and Regulatory Technical Standards) are implemented as appropriate so that customers can be assured that the Director implements robust anti-fraud measures in order to best protect their funds and personal information.	The Supplier shall ensure that any new regulatory requirements relating to customers or their proxies accessing online banking services (including but not limited to Strong Customer Authentication and Regulatory Technical Standards) are implemented as appropriate so that customers can be assured that the Director implements robust anti-fraud measures in order to best protect their funds and personal information.
PPC-L3-SEC-302	PPCL2-SEC-003	**Security**	The supplier shall ensure that any actions taken in response to authentication failures make use of a cumulative fail count across all channels so that a potential malicious actor is prevented from working their way through the channels to gain access.	The supplier shall ensure that any actions taken in response to authentication failures make use of a cumulative fail count across all channels so that a potential malicious actor is prevented from working their way through the channels to gain access.
PPC-L3-SEC-303	PPCL2-SEC-003	**Security**	The Supplier shall ensure that at least one copy of the backup of Director Data is held offline at any one time, so that the system can always be restored from backup in the event of a successful ransomware or other relevant malicious software attack.	The Supplier shall ensure that where multiple alternative methods of authentication are available to customers to access their accounts, they do not increase the overall risk to the Director or the customer so that the Directors risk profile remains consistent across channels.
PPCL3-TRF-006	PPCL2-TRF-001	**Transformation**	he strategy shall include timelines and anticipated milestones to incrementally achieve a higher take up rate in self - service by customers, so that the Director can be kept informed on the progress of the strategy versus plan	
PPCL3-TRF-007	PPCL2-TRF-001	**Transformation**	Following the Director's approval of the strategy and an agreed established baseline , the Supplier shall adopt and execute against its agreed strategy, so that it can achieve agreed customer digital self service take up targets on behalf of the Director.	
PPCL3-TRF-008	PPCL2-TRF-001	**Transformation**	The supplier shall work with the Directors communication team, so that migration activities	
PPCL3-TRF-009	PPCL2-TRF-001	**Transformation**	The strategy shall demonstrate how risks and the proposed remediations to take will be tracked, so that the Director can be assured of a successful migration	
PPCL3-TRF-010	PPCL2-TRF-001	**Transformation**	Roles, responsibilities and interdependencies to deliver the strategy across the Supplier, Director and other parties should be included so that the Director can be informed of the resourcing and organisation dedicated to the Digital Migration programme.	
PPCL3-TRF-011	PPCL2-TRF-001	**Transformation**	Following the Director's approval of the strategy and an agreed established baseline , the Supplier shall adopt and execute against its agreed strategy, so that it can achieve agreed customer digital self service take up targets on behalf of the Director.	
PPCL3-TRF-012	PPCL2-TRF-001	**Transformation**	The Supplier will propose, develop and regularly deliver metrics, to monitor and report the take up rate of self-service by customers whilst monitoring that high quality and timely customer experience is maintained.	
PPC-L3-SEC-304	PPCL2-SEC-002	**Security**	The solution shall ensure that any co-browsing activity is read-only and shall not allow any direct control of customer browsing sessions or cause changes to customer browser screens.	The Supplier shall ensure that the use of all Cloud Services within their Solution complies with the Directors Cloud Security Standard, so that Director can be assured that the solution meets the Directors Risk Appetite
PPC-L3-SEC-305	PPCL2-SEC-002	**Security**	The Supplier shall only undertake co-browsing activities after the customer has provided consent to an authenticated customer agent.	New Requirement
PPC-L3-SEC-306	PPCL2-SEC-002	**Security**	The Supplier shall design its security architecture and controls in accordance with the NCSC's Zero-Trust design principles, so that that there is high assurance in the security of the solution through a defence-in-depth approach.	New Requirement

SCHEDULE 2.2 - PERFORMANCE LEVELS

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

Available means when, in respect of the IT Environment and/or the Services:

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

b) the Supplier System is able to process the Director Data in accordance with the Services Description including providing such reports as are required within the timescales specified (as measured on a 24 x 7 basis); and

c) all Performance Indicators other than Customer Systems Availability are above the KPI Service Threshold,

and **Availability** shall be construed accordingly.

Customer Systems Availability and Performance shall be measured as a percentage of the total time in a Service Period (in respect of Availability) or as otherwise calculated (for Performance) in accordance with the formula set out in KPI9 (Customer Systems Availability) and as detailed in Annex 1 of of this Schedule.

Dashboard means the provision of a live dashboard allowing the Director to access performance and Incident management information in real time.

Incident has the meanings given in the definitions of P1 – P4 incidents as set out in Paragraph 2 of Annex 1.

Non-Available means in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available.

Performance Monitoring Report has the meaning given in Paragraph 1.2 of Part 2.

Performance Review Meeting means the regular meetings between the Supplier and the Director to manage and review the Supplier's performance under this Agreement, as further described in Paragraph 1.5 of Part 2.

Permanent Fix means in relation to an Incident, an agreed technical solution, which is not a workaround, which will prevent the event which caused the original Incident from re-occurring.

Repeat KPI Failure has the meaning given in Paragraph 3 of Part 1.

Resolved means in relation to an Incident, either a Permanent Fix has been deployed or, if not possible, a workaround is deployed in accordance with the provisions of Paragraph 3.1 of Part 2.

Service Downtime means any period of time during which any of the Services are not Available and for the avoidance of doubt shall include where not Available due to Permitted Maintenance.

Part 1: PERFORMANCE INDICATORS AND SERVICE CREDITS

1 PERFORMANCE INDICATORS

1.1 Annex 1 sets out the Key Performance Indicators and Subsidiary Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

1.2 The Supplier shall monitor its performance against each Performance Indicator and shall send the Director a report detailing the level of service actually achieved in accordance with Part 2.

1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2, 3 and 4.

2 SERVICE POINTS

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

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

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

3 REPEAT KPI FAILURES AND RELATED KPI FAILURES

Repeat KPI Failures

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

3.2 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure that is a Repeat KPI Failure shall be calculated as follows:

SP = P x 2

where:

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

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

Related KPI Failures

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

4 SERVICE CREDITS

4.1 Schedule 7.1 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.

4.2 The Director shall use the Performance Monitoring Reports provided pursuant to Part 2, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

5 PERFORMANCE RELIEF DUE TO PERFORMANCE OF INCUMBENT

5.1 Notwithstanding and without prejudice to the Director's rights and remedies under this Agreement, where a key performance indicator ("Legacy KPI") under the Legacy Service Contract between the Director and the Former Supplier has a service level target for a specific Legacy KPI that has not been met by the Former Supplier to Level 3 Performance Threshold standard (as defined within the Legacy Service Contract) or worse for three (3) consecutive months prior to the relevant Operational Service Commencement Date for an equivalent Service under this Agreement, the Director will consider the grant of relief to the Supplier (the granting of such relief not to be unreasonably withheld). The relief will take the form of not deducting Service Credits in accordance with the mechanism set out in Schedule 7.1 (*Charges and Invoicing*) for the equivalent Key Performance Indicator set out in Annex 1 of this Schedule 2.2 (*Performance Levels*) (a "Service Credit Holiday") for a period of up to a maximum of three (3) months from the relevant Operational Service Commencement Date for the respective Service and may be subject to conditions to be agreed between the Parties specific to the circumstances.

5.2 Notwithstanding Paragraph 5.1, all other remedies available to the Director, including as set out in this Agreement and this Schedule 2.2 (*Performance Levels*) will remain applicable and Service Points shall continue to accrue.

6 PERFORMANCE RELIEF ON TRANSITION

6.1 The Supplier shall deliver against the Key Performance Indicators/Subsidiary Performance Indicators', from the point at which the Supplier is responsible for delivering an element of the Service at the identified Operational Service Commencement Date or such other "go live" date (as set out in the Implementation Plan). The Service Credit regime referenced in Paragraph 4.1 of Part 1 of this Schedule 2.2 (*Performance Levels*) will apply immediately the relevant Operational Services commence.

6.2 Table 1 (KPI relationship to Implementation Plan) shows the Key Performance Indicator's that are applicable following the first, second and third Operational Service Commencement Dates which are indicated by the letter 'N' if the KPI/PI is not applicable and the letter 'Y' if it is applicable during the Service Period following the respective Operational Service Commencement Date. Following the third Operational Service Commencement Date all Key Performance Indicators/Subsidiary Performance Indicators' will be applicable. Measures 1.5, 1.6.1 and 1.6.2 are new measures not reflected in the Legacy Service Contract and will be agreed between the parties prior to the second OSCD.

6.3 Notwithstanding and without prejudice to the Director's rights and remedies under this Agreement, the Supplier may submit a request for relief in respect of the specific Performance Indicators as set out in Table 1 (KPI relationship to Implementation Plan) of this Paragraph 6 and the Director acting at its sole discretion will grant the appropriate relief. The potentially impacted KPI's are shown in Table 1 (KPI relationship to Implementation Plan) in each column by the use of a '**Y***' letter combination below.

Table 1 – KPI Relationship to Implementation Plan

No	KPI/PI title and short description	from first OSCD	from second OSCD	from third OSCD
1.1	Average Speed Answer	Y*	Y*	Y
1.2	Abandoned Rate	Y*	Y*	Y

1.3	Timeliness	Y*	Y*	Y
1.4	Accuracy	Y*	Y*	Y
1.5	First Contact Resolution	N	Y*	Y
1.6.1	Customer Satisfaction (human)	N	Y	Y
1.6.2	Customer Satisfaction (virtual)	N	Y*	Y
2.1	Sales confirmation documentation	Y*	Y	Y
2.2	% of cheques scanned and uploaded to Deposit system	N	Y	Y
2.3	% requests for further information or clarification	Y*	Y*	Y
2.4	% Legal documents sent to the Customer	Y*	Y*	Y
2.5	% requests for information or clarification sent to the Customer	Y*	Y*	Y
2.6	% requests for Evidence of Identity required to process a sale	Y*	Y*	Y
2.7	% funds instructed to be returned to the Customer	Y*	Y*	Y
3.1	% responses providing resolution to Customer queries	Y*	Y*	Y
3.2	% Customer Records updated	Y*	Y*	Y
3.3	% searches requested via My Lost Account	Y*	Y*	Y
3.4	% Death Claim full responses or requests for further information	Y*	Y*	Y
3.5	% of Customer requests to register for telephony and online	Y*	Y*	Y
3.6	% of Forgotten Security responded to within two (2) Working Days	Y*	Y*	Y
4.1	% all complaints Resolved and closed	Y*	Y*	Y
4.2	% complaints recognised as a complaint at 1st contact	Y*	Y*	Y
4.3	% all complaints Resolved and closed by the third day	Y*	Y*	Y
4.4.1	Complaints relating to PPC Supplier error upheld by FOS	Y*	Y*	Y
4.4.2	Number of all complaints upheld by FOS	Y*	Y*	Y
4.5	% complaints in which we receive a second reply	Y*	Y*	Y
5.1	Document Creation	N	Y*	Y
6.1	Print and Post Out – Prize Warrants	N	Y*	Y
6.2	Print and Post Out – “Daily Files”	N	Y*	Y
6.3	Print and Post Out – Scheduled Statements	N	Y*	Y
7.1	Data Subject Rights Requests	Y	Y	Y
7.2	Compliance Training - New Starters	Y	Y	Y
7.3	Compliance Training - Refresher	Y	Y	Y
7.4	Open actions related to audit and compliance	Y*	Y*	Y
8.1	Customer data capture and verification	Y*	Y*	Y
8.2	Financial Crime Investigations	Y*	Y*	Y
9.1	Availability Documents View	N	Y*	Y
9.2	Documents View response performance	N	Y*	Y
9.3	Availability: Contact Centre Servicing Solutions	Y*	Y*	Y
9.4	Availability: Customer Servicing Solutions	Y*	Y*	Y
9.5	Performance: Customer Servicing Solutions	Y*	Y*	Y
9.6	Performance: Co Browsing Solution response performance	N/A	N/A	N/A
10.1	Critical Vulnerability Patches Deployed	Y**	Y**	Y
10.2	High, Medium and Low Vulnerability Patches Deployed	Y**	Y**	Y
11.1	P1 Initial Incident Resolution Time	Y**	Y**	Y
11.2	P2 Initial Incident Resolution Time	Y**	Y**	Y
11.3	P3 Initial Incident Resolution Time	Y**	Y**	Y
11.4	P4 Initial Incident Resolution Time	Y**	Y**	Y
11.5	P1 Incident Root Cause Analysis	Y**	Y**	Y
11.6	P2 Incident Root Cause Analysis	Y**	Y**	Y
11.7	P3 Incident Root Cause Analysis	Y**	Y**	Y
11.8	P4 Incident Root Cause Analysis	Y**	Y**	Y
11.9	Permanent Fix Availability	Y**	Y**	Y
11.10	Permanent Fix Deployment	Y**	Y**	Y
11.11	Post Release Incident Rate	Y**	Y**	Y
12.1	P1 Incident Communication Time	Y**	Y**	Y
12.2	P2 Incident Communication Time	Y**	Y**	Y

The respective KPIs within Table 1 above will become effective when the Test Certification or Milestone Achievement Certificate (as applicable) has been issued in relation to the relevant Deliverable or Milestone associated with the respective Services.

The KPIs marked Y in Table 1 will measure the performance of Supplier Systems and Services only. In other words these KPI's will be applicable once the Supplier Systems are implemented and the Supplier is carrying out the activities indicated by the KPI/PI on the respective system.

6.4 At the Director's sole discretion, if:

6.4.1 the performance requirements of the relevant Performance Indicators are more onerous than the equivalent provisions under the Legacy Service Contract; and

6.4.2 the Implementation Plan justifies relief;

the Director may grant relief in the form of holding in abeyance the deduction of Service Credits in the event the failure to deliver a Key Performance Indicator/Subsidiary Performance Indicator has not been possible because of a failure of the service (or part of the service) provided by the Former Supplier which has had an impact on the KPI achievement by the Supplier. Such relief shall not exceed a maximum of three (3) months from the relevant Operational Service Commencement Date unless otherwise agreed between the parties.

6.5 Notwithstanding Paragraphs 6.1 to 6.4, all other remedies available to the Director, including as set out in this Agreement and this Schedule 2.2 (*Performance Levels*) will remain applicable and Service Points will continue to accrue. Following the third Operational Service Commencement Date the Supplier will no longer have the right to request relief pursuant to Paragraph 6.3. The Director accepts and agrees that performance information presented prior to the completion of Milestone MS13 (the third Operational Service Commencement Date) is dependent on the Supplier's ability to obtain the information from the Former Supplier and the information may therefore be missing, not aligned to the measures used in this Agreement, incomplete or inaccurate.

Part 2: PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 In addition to any information provided as part of the Dashboard reporting requirements in Schedule 8.4 (*Reports and Records Provisions*), the Supplier shall provide live performance monitoring information against each Performance Indicator for display on the Dashboard.

1.2 Notwithstanding the information provided as part of the Dashboard, within ten (10) Working Days of the end of each Service Period, the Supplier shall also provide a report to the Director Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.3 (the "**Performance Monitoring Report**").

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

Information in respect of the Service Period just ended

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

1.3.2 a summary of all Performance Failures that occurred during the Service Period;

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

1.3.4 which Performance Failures remain outstanding and progress in resolving them;

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

1.3.6 the status of any outstanding Rectification Plan processes, including:

(a) whether or not a Rectification Plan has been agreed; and

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

1.3.7 the status of any Incident where a root cause analysis is being (or has been) undertaken and action taken or planned to resolve the underlying cause and prevent recurrence;

1.3.8 a list of any workarounds still in place on the last day of the Service Period and the status of any proposed resolution to remove the workaround;

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

1.3.10 the number of Service Points awarded in respect of each KPI Failure;

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

1.3.12 the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

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

1.3.14 such other details as the Director may reasonably require from time to time; and

Information in respect of previous Service Periods

1.3.15 a rolling total of the number of Performance Failures that have occurred over the past six (6) Service Periods;

1.3.16 the amount of Service Credits that have been incurred by the Supplier over the past six (6) Service Periods;

1.3.17 the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

Information in respect of the next Quarter

1.3.18 any scheduled Permitted Maintenance and Updates that have been agreed between the Director and the Supplier for the next Quarter.

1.4 The Performance Monitoring Report shall be reviewed and its contents agreed by the Parties at the next Supplier Delivery and Supplier Management Committee held in accordance with Paragraph 1.5.

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

1.5.1 take place within five (5) Working Days of the Performance Monitoring Report being issued by the Supplier;

1.5.2 take place at such location and time (within normal business hours) as the Director shall reasonably require (unless otherwise agreed in advance); and

1.5.3 be attended by the Supplier Representative and the Director Representative.

1.6 The Director shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure and/or PI Failure.

2 CLOCK STOP

2.1 The Supplier's obligation to resolve or respond to an Incident in accordance with Key Performance Indicator's 11.1 -11.4 shall be suspended for any period of Clock Stop applied to that specific Incident.

2.2 A Clock Stop can only occur in the following circumstances:

2.2.1 where the Incident is passed to a third party that is not within the control of the Supplier or for which the Supplier has responsibility for;

2.2.2 where the Supplier, acting reasonably has passed control of the Incident to the Director or a Relevant Third Party Supplier for resolution; or

2.2.3 by mutual agreement with the Director.

3 WORKAROUNDS

3.1 Where a workaround in respect of an Incident is identified and the Director deems such workaround acceptable and it is deployed:

3.1.1 the relevant Incident shall be deemed Resolved for the purposes of KPI's 11.1 – 11.4 below; and

3.1.2 that workaround shall be formally recorded in a central database which shall be held and maintained in the Virtual Library.

3.2 Notwithstanding the above, all workarounds shall be Resolved in accordance with KPI 11.9 (Permanent Fix Availability) and KPI 11.10 (Permanent Fix Deployment). The Director shall review and approve the proposed remediation acting reasonably. No remedial work shall be deployed without approval of the Director and subject to relevant Testing pursuant to Schedule 6.2 (*Testing Procedures*).

3.3 Where a workaround is remediated and the workaround is no longer used, the central workaround database on the Virtual Library shall be updated accordingly.

4 PERFORMANCE RECORDS

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

4.2 In addition to the requirement in Paragraph 4.1 to maintain appropriate documents and records, the Supplier shall provide to the Director such supporting documentation as the Director may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.

4.3 The Supplier shall ensure that the Performance Monitoring Report (as well as historic Performance Monitoring Reports) and any variations or amendments thereto, any reports and summaries produced in accordance with this Schedule and any other document or record reasonably required by the Director are available to the Director on-line and are capable of being printed.

5 PERFORMANCE VERIFICATION

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

6 VIRTUAL LIBRARY COMPLETENESS

6.1 The Virtual Library shall be complete where all of the information required under Schedule 8.4 (*Reports and Records Provisions*) Annex 3 (*Record to Upload to Virtual Library*) has been uploaded to the Virtual Library in accordance with Paragraph 3 of that Schedule.

ANNEX 1: KEY PERFORMANCE INDICATORS AND PERFORMANCE INDICATORS

Part 1: KEY PERFORMANCE INDICATORS AND SUBSIDIARY PERFORMANCE INDICATORS TABLES

1. The Key Performance Indicators (KPI) and Subsidiary Performance Indicators (PI) that shall apply to the Operational Services are set out below:

KPI 1 – Contact Centre - Assisted Digital (Telephone, Social Media, Web chat)					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
1.1	Average Speed Answer: 80% calls answered within 60 seconds from when the Customer selects an option on the IVR to speak with an Agent.	80% of all calls delivered via the telephone switch into the Contact Centre, once the Customer has made their relevant IVR selection choice, will be answered by an Agent within 60 seconds of waiting.	Target Performance Level	80%	0
			Minor KPI Failure	78%	5
			Serious KPI Failure	75%	12
			Severe KPI Failure	65%	20
			KPI Service Threshold	60%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
1.2	Abandoned Rate: No more than 5% of inbound calls abandoned from when the Customer selects an option on the IVR to speak with an Agent.	No more than 5% of all calls delivered via the Telephone switch into the Contact Centre, will be abandoned once the Customer has made their relevant IVR selection choice.,	Target Performance Level	5%	0
			Minor KPI Failure	7%	5
			Serious KPI Failure	9%	12
			Severe KPI Failure	11%	20
			KPI Service Threshold	13%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**

1.3	Timeliness: % replies sent to the Customer within the expected timescale for that Channel.	97% of Customer enquiries will be reviewed and responded to (if appropriate), within the following timescales, after they are detected on the relevant platform. Webchat (incl In App) 40 seconds Email 24 hrs Secure Message (incl In App) 24hrs Twitter 30 minutes Facebook 1 hour	Target Performance Level	97%	0
			Minor KPI Failure	96.99%	3
			Serious KPI Failure	90% Timeliness	6
			Severe KPI Failure	85% Timeliness	10
			KPI Service Threshold	75%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
1.4	Accuracy: % responses to Customer's contacts are accurate across all written Channels.	Responses to Customers must be accurate. Webchat (incl In App) Email Secure Message Twitter Facebook The criteria to be used to check for accuracy are: 1. Correct spelling, grammar & formatting 2. Security procedure adhered to and compliance 3. Identifying and understanding the query 4. Communication and Tone of voice 5. Accurate and relevant information given.	Target Performance Level	97%	0
			Minor KPI Failure	96.99%	3
			Serious KPI Failure	90% Accuracy	6
			Severe KPI Failure	85% Accuracy	10
			KPI Service Threshold	75%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI/KPI title and short description**	**PI/KPI Definition**	**Severity levels**		**Service points**
1.5	First Contact Resolution: Customers will be able to complete their jobs to be done at the first time of asking.	Phone – % Chat (Web or InApp) - % Email – % Secure Message – % Twitter – % Facebook N/A TBA – targets may vary by channel	Target Performance Level	TBC%	0
			Minor KPI Failure	% Satisfaction	3
			Serious KPI Failure	% Satisfaction	6
			Severe KPI Failure	% Satisfaction	10
			KPI Service Threshold	< %	15
Reporting and measurement			**Inclusions and exclusions**		

Frequency of measurement: Monthly		Commence as PI, establish appropriate Service thresholds in accordance with Clause 7.8 of the front end terms & trigger as KPI after relevant OSCD taking into account the relevant review of performance track record.	TBA – targets may vary by channel	
No	**KPI title and short description**	**KPI Definition**	**Severity levels**	**Service points**
1.6.1	Customer Satisfaction: The Customer's satisfaction of a "Human" Agent's service.	Phone –% Chat (Web or InApp)- % Email – % Secure Message – % Twitter – % Facebook N/A Commence as PI, establish appropriate Service thresholds in accordance with Clause 7.8 of the front end terms & trigger as KPI after relevant OSCD taking into account the relevant review of performance track record – nb: these may vary by channel	Target Performance Level: TBC%	0
			Minor KPI Failure: % Satisfaction	5
			Serious KPI Failure: % Satisfaction	12
			Severe KPI Failure: % Satisfaction	20
			KPI Service Threshold: < %	30
Reporting and measurement **Frequency of measurement:** Monthly			**Inclusions and exclusions** TBA – targets may vary by channel	
No	**KPI title and short description**	**KPI Definition**	**Severity levels**	**Service points**
1.6.2	Customer Satisfaction: The Customer's satisfaction of a Virtual Agent's service.	Phone – % Chat (Web or InApp)- % Email –% Secure Message – % Twitter – % Facebook N/A Commence as PI, establish appropriate Service thresholds in accordance with Clause 7.8 of the front end terms & trigger as KPI after relevant OSCD taking into account the relevant review of performance track record – nb: these may vary by channel	Target Performance Level: TBC %	0
			Minor KPI Failure: % Satisfaction	5
			Serious KPI Failure: % Satisfaction	12
			Severe KPI Failure: % Satisfaction	20
			KPI Service Threshold: < %	30
Reporting and measurement **Frequency of measurement:** Monthly			**Inclusions and exclusions** TBA – targets may vary by channel	

KPI 2 – Sales & Payments					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
2.1	% Sales confirmation documentation provided to the Customer within two (2) Working Days of receipt of an acceptable sales application received by post.	The Supplier shall process the sale within two (2) Working Days of receipt of the acceptable sales application received by post. Timeliness & Accuracy shall be measured providing a combined performance result against the target performance level/threshold.	Target Performance Level	97%	0
			Minor KPI Failure	96%	1
			Serious KPI Failure	93%	2
			Severe KPI Failure	90%	3
			KPI Service Threshold	85%	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
2.2	% of cheques received by 1pm, including those from any previous Working Day, that are scanned and uploaded to the Remote Cheque Deposit system provided by the Out-Clearing Service Provider on that day by a time agreed by the Director and of debit card payments processed immediately during a Working Day (subject to the reporting cut off of the system at 23:45pm with payments processed after showing on the next Working Day).	The Supplier shall, where a sales application and cheque or warrant are received by post before 1pm on a Working Day, or have been received and carried forward from the previous Working Day, prepare, collate, reconcile, scan & upload images of the cheques or warrants on the same Working Day by a time agreed by the Director onto the Remote Cheque Deposit system provided by the Out-Clearing Service Provider. The cheques and warrants shall be kept for thirty (30) Working Days before being confidentially destroyed. Timeliness shall be measured providing a performance result against the target performance level/threshold.	Target Performance Level	97%	0
			Minor KPI Failure	96%	1
			Serious KPI Failure	93%	2
			Severe KPI Failure	90%	3
			KPI Service Threshold	85%	4
Reporting and measurement			**Inclusions and exclusions**		

Frequency of measurement: Monthly		

No	KPI title and short description	KPI Definition	Severity levels		Service points
2.3	% requests for further information or clarification required to process a sale sent to the Customer within four (4) Working Days of receipt of a sales application sent by post.	The Supplier shall, in the event that a sales application received by post has been accepted, and it is subsequently discovered that further information or clarification is required in order to process the sales application or its corresponding funds, contact the Customer within four (4) Working Days of receipt of the sales application to request such information or clarification. On receipt of further information or clarification from the Customer, the Supplier shall process the acceptable sales application.	Target Performance Level	97%	0
			Minor KPI Failure	96%	1
			Serious KPI Failure	93%	2
			Severe KPI Failure	90%	3
			KPI Service Threshold	85%	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

No	PI title and short description	PI Definition	Severity levels		Service points
2.4	% legal documents sent to the Customer securely within two (2) Working Days of receipt.	The Supplier shall receive, validate and register the Customers legal documents. The Supplier/Provider shall return the legal documents to the Customer using a secure method having regard to the nature of the legal documents within two (2) Working Days of receipt, together with a covering letter of acknowledgement.	Target Performance Level	97%	0
			Minor KPI Failure	96%	1
			Serious KPI Failure	93%	2
			Severe KPI Failure	90%	3
			KPI Service Threshold	85%	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

No	KPI title and short description	KPI Definition	Severity levels		Service points
2.5	% requests for information or clarification sent to the Customer within three (3) Working Days of a postal	The Supplier shall, where the Supplier requires further information or clarification in relation to a postal payment application, contact the Customer within three (3) Working Days seeking such information or clarification and once	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10

	payment application for which further information is required.	sufficient information is received, shall process the acceptable payment application in accordance with the payment process.	KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
2.6	% requests for Evidence of Identity required to process a sale sent to the Customer within two (2) Working Days of receipt of a sales application received by post.	The Supplier shall, in the event that a sales application received by post has been accepted, and it is subsequently discovered that Evidence of Identity information or clarification is required in order to process the sales application or its corresponding funds, contact the Customer within two (2) Working Days of receipt of the sales application to request the Evidence of Identity information or clarification. On receipt of valid/authenticated information or clarification from the Customer, the Supplier shall process the acceptable sales application.	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
2.7	% funds instructed to be returned to the Customer's original source of funds within two (2) Working Days of receipt of an unacceptable Sales Application, an unacceptable cheque or the Customer request to cancel the application.	The Supplier shall reject any sales application received by post from the Customer, where the Product or Product term is not currently Available, or where the subscription limits for tranches have been reached. In such cases, the Provider shall return the sales application and associated funds to the Customer together with a letter of explanation within two (2) Working Days of the date of receipt. The Supplier will reject any unacceptable cheque received from the Customer. A written explanation for such rejection shall be enclosed with the unacceptable cheque and despatched to the Customer within two (2) Working Days of the date of receipt.	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

	The Supplier shall, in the event that the Customer decides to cancel a sale within the cooling off period, cancel the sale, update the Customer record (the Core Banking, Payments & Reporting provider will then return any funds provided by the Customer to the Customer together with any interest due), within (two) 2 Working Days of receiving notice of request for cancellation from the Customer or, if the funds have not cleared, within (two) 2 Working Days of the funds clearing.	

KPI 3 – Servicing					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
3.1	% responses providing resolution to Customer queries received by post sent to within four (4) Working Days of receipt.	The Supplier shall ensure that when a query relating to their Account is received by post from an authenticated customer, the Supplier shall send a response providing them with a resolution to their query. The responses shall be sent within four (4) Working Days of receipt.	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
3.2	% Customer Records updated within three (3) Working Days of receipt of a valid instruction for a change of personal or bank details received by post and, for change of address, confirmation sent to the Customer by the Customer's stated communication method.	The Supplier shall, where a Product allows management by post: receive postal instructions from the Customer for a change of personal or bank details and confirm to the Customer within three (3) Working Days of receipt of the change of details that the change has been effected to the Customer Record.	Target Performance Level	98.5%	0
			Minor KPI Failure	97%	1
			Serious KPI Failure	94%	2
			Severe KPI Failure	91%	3
			KPI Service Threshold	85%	4

Reporting and measurement			Inclusions and exclusions		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
3.3	% searches requested via My Lost Account or the NS&I Tracing Service completed within twenty (20) Working Days of receipt of Customer query.	The Supplier shall, in the event that a Customer requests the Supplier to trace an account via the NS&I Tracing Service or My Lost Account service: complete a search of all Customer Records and confirm to the Customer whether or not they still have an Account, within twenty (20) Working Days of receiving the request.	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
3.4	% Death Claim full responses or requests for further information despatched within seven (7) Working Days of receipt of correspondence or enquiry.	The Supplier/Provider shall deal with all Death Claims sensitively and in accordance with guidance issued by the Financial Conduct Authority (FCA) and the British Banking Association (BBA) and provide a full response or request for further information within seven (7) Working Days of receipt of correspondence or enquiry.	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
3.5	% of Customer requests to register for telephony and online services received by post, on-line form or as a consequence of the Customer not fully/successfully completing the digital journey	The Supplier/Provider shall successfully process Customer requests to register for telephony and online services received by post or as a consequence of the Customer not fully/successfully completing the digital journey process, to be processed and Customer	Target Performance Level	97%	0
			Minor KPI Failure	96%	3
			Serious KPI Failure	93%	6
			Severe KPI Failure	90%	10
			KPI Service Threshold	85%	15

	process, to be processed and customer responded to within four (4) Working Days of receipt of the Customer request.	responded to within four (4) Working Days of receipt of the Customer request.			
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
3.6	% of Forgotten Security requests received by post or on-line form to be processed and the customer responded to within two (2) Working Days of receipt of Customer request.	The Supplier/Provider shall successfully process Customer requests to resolve Forgotten Security correspondence/requests received from the Customer by post or as a consequence of the Customer not fully/successfully completing the digital journey process, to be processed and customer responded to within two (2) Working Days of receipt of the Customer request.	Target Performance Level	97%	0
			Minor KPI Failure	96%	5
			Serious KPI Failure	93%	12
			Severe KPI Failure	90%	20
			KPI Service Threshold	85%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 4 – Complaints					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
4.1	% all complaints Resolved and closed that have been handled as set out in the FCA Handbook.	% all complaints Resolved and closed that have been handled as set out in the FCA Handbook.	Target Performance Level	99%	0
			Minor KPI Failure	98%	5
			Serious KPI Failure	96%	12
			Severe KPI Failure	92%	20
			KPI Service Threshold	90%	30
Reporting and measurement			**Inclusions and exclusions**		

Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
4.2	% complaints recognised as a complaint at 1st point of contact.	% complaints recognised as a complaint at 1st point of contact.	Target Performance Level	99%	0
			Minor KPI Failure	98%	5
			Serious KPI Failure	96%	12
			Severe KPI Failure	92%	20
			KPI Service Threshold	90%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
4.3	% all complaints Resolved and closed by the third business day following the day on which it is received (four (4) business days) as required by FCA DISP1 (Dispute Resolution: Complaints).	The percentage of all complaints Resolved and closed by the third business day following the day on which it is received (four (4) business days) as required by FCA DISP1 (Dispute Resolution: Complaints).	Target Performance Level	75%	0
			Minor KPI Failure	<75%	3
			Serious KPI Failure	65%	6
			Severe KPI Failure	<55%	10
			KPI Service Threshold	<50%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
4.4.1	Number of all complaints relating to PPC Supplier error upheld by FOS.	The number of all complaints relating to PPC Supplier error upheld by FOS. This will be calculated on the upheld cases received from The Financial Ombudsman Service on a monthly basis.	Target Performance Level	4 Cases	0
			Minor KPI Failure	5 Cases	1
			Serious KPI Failure	6 Cases	2
			Severe KPI Failure	8 Cases	3
			KPI Service Threshold	10 Cases	4

Reporting and measurement			Inclusions and exclusions		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
4.4.2	Number of all complaints upheld by FOS based upon the following: Average monthly calculated over the twelve (12) preceding months.	Number of all complaints upheld by FOS based upon the following: Average monthly calculated over the twelve (12) preceding months.	Target Performance Level	4 Cases	0
			Minor KPI Failure	5 Cases	1
			Serious KPI Failure	6 Cases	2
			Severe KPI Failure	8 Cases	3
			KPI Service Threshold	10 Cases	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
4.5	% of complaints in which we receive a second uninvited negative reply from the Customer in relation to the final response letter.	% all complaints Resolved and closed whereby a Customer provides an uninvited negative reply off the back of issuing our final response letter.	Target Performance Level	>20%	0
			Minor KPI Failure	>30%	3
			Serious KPI Failure	>35%	6
			Severe KPI Failure	>40%	10
			KPI Service Threshold	>50%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 5 – Document Management & Creation				
No	**PI title and short description**	**PI Definition**	**Severity levels**	**Service points**

5.1	Document Creation.	The Supplier shall on receipt of a document creation instruction immediately construct, “store” and make available the accurately formatted and populated document.	Target Performance Level	100% within 5000ms	0
			Minor KPI Failure	<100% within 5000ms	1
			Serious KPI Failure	<99.9% within 5000ms	2
			Severe KPI Failure	<99.8% within 5000ms	3
			KPI Service Threshold	99.7% within 5000ms	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 6 – Print & Despatch					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
6.1	Print & Post Out – Prize Warrants.	The Supplier shall on receipt of a Post Out trigger instruction ensure that all relevant documents are accurately printed, enclosed with any additional “fulfilments” and dispatched within seven (7) working days of trigger receipt.	Target Performance Level	100%	0
			Minor KPI Failure	99.99%	5
			Serious KPI Failure	99.95%	12
			Severe KPI Failure	99.90%	20
			KPI Service Threshold	99.80%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**

6.2	Print & Post Out – “Daily Files”.	The Supplier shall on receipt of a Post Out trigger instruction which is received before [xx:xx] hrs (to be determined in accordance with Clause 7.8 of the Agreement and subject to identified dependencies on detailed design in relation to other Relevant Third Party Suppliers, including the banking engine) ensure that all relevant documents are accurately printed, enclosed with any additional “fulfilments” and dispatched the same Working Day. Trigger instruction events received after this time will be dispatched the following Working Day.	Target Performance Level	100%	0
			Minor KPI Failure	99.99%	5
			Serious KPI Failure	99.95%	12
			Severe KPI Failure	99.90%	20
			KPI Service Threshold	99.80%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
6.3	Print & Post Out – Scheduled Statements.	The Supplier shall on receipt of a Post Out trigger instruction ensure that all relevant documents are accurately printed, enclosed with any additional “fulfilments” and dispatched within seven (7) Working Days of trigger receipt.	Target Performance Level	100%	0
			Minor KPI Failure	99.99%	1
			Serious KPI Failure	99.95%	2
			Severe KPI Failure	99.90%	3
			KPI Service Threshold	99.80%	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 7 – Compliance				
No	**KPI title and short description**	**KPI Definition**	**Severity levels**	**Service points**

7.1	Data Subject Rights Requests.	% of valid Data Subject Rights Requests completed/fulfilled within regulatory timescales (currently one (1) calendar month).	Target Performance Level	100%	0
			Minor KPI Failure	99%	5
			Serious KPI Failure	97%	12
			Severe KPI Failure	95%	20
			KPI Service Threshold	90%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**Definition**	**Severity levels**		**Service points**
7.2	Compliance Training - New Starters.	% of new staff completing compliance training including (DPA, AML, BCOBs, FOI and Complaints) within one (1) month of starting date (less any who leave within one (1) month).	Target Performance Level	100%	0
			Minor KPI Failure	99%	5
			Serious KPI Failure	97%	12
			Severe KPI Failure	95%	20
			KPI Service Threshold	90%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**Definition**	**Severity levels**		**Service points**
7.3	Compliance Training – Refresher.	% of staff (excluding those on extended absence) completing compliance training including (DPA, AML, BCOBs, FOI and Complaints) within one (1) month of due date for refresher training.	Target Performance Level	98%	0
			Minor KPI Failure	97%	3
			Serious KPI Failure	95%	6
			Severe KPI Failure	93%	10
			KPI Service Threshold	85%	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**Definition**	**Severity levels**		**Service points**

7.4	<u>Audit and Compliance Actions:</u> Open actions related to audit and compliance.	The number of audit and remedial actions, including but not limited to, Compliance, Security, Business Continuity that remain open one (1) month or more past agreed due date.	Target Performance Level	Zero (0) actions open past agreed due date.	0
			Minor KPI Failure	One (1) or more actions open past agreed due date.	3
			Serious KPI Failure	Three (3) or more actions open past agreed due date, OR One (1) or more action open longer than one (1) month past agreed due date.	6
			Severe KPI Failure	Five (5) actions or more actions open past agreed due date, OR One (1) or more action open longer than two (2) months past agreed due date.	12
			KPI Service Threshold	Ten (10) actions open past agreed due date, OR One (1) or more action open longer than three (3) months past agreed due date.	15
Reporting and measurement			**Inclusions and exclusions**		
<u>Frequency of measurement:</u> Monthly					

KPI 8 – Financial Crime				
No	**KPI title and short description**	**KPI Definition**	**Severity levels**	**Service points**

8.1	Customer data capture and verification.	Customers mandatory details are captured in every application and validated as and when details are changed. • *bank account verification matches during on-boarding* • *impersonation checks performed during application* • *initial customer screening undertaken in real-time*	Target Performance Level	100%	0
			Minor KPI Failure	n/a	-
			Serious KPI Failure	99%	12
			Severe KPI Failure	95%	20
			KPI Service Threshold	90%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly			At the end of the reporting period (monthly), Service Provider (SP) must provide Service Recipient (SR) the number of ID&V checks performed, the number of passed & failed ID&V checks, number of escalated cases, backlog of escalated and age of each escalated case.		
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
8.2	Financial Crime Investigations.	• Payments paused by the risks controls needs to be investigated and approved by next Working Day. • Investigation needs to be triaged and worked on within the agreed timescale defined by the Director. • DAML SARs need to be triaged, raised and submitted by the end of the following day.	Target Performance Level	100%	0
			Minor KPI Failure	99%	5
			Serious KPI Failure	95%	12
			Severe KPI Failure	90%	20
			KPI Service Threshold	85%	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 9 – Customer Systems Availability & Performance					
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
9.1	Availability Documents View :	The Document View/store service shall be Available 99.99% of its operating hours to	Target Performance Level	99.99% Availability	0

<table>
<tr><td></td><td>The availability of the Documents viewing services to enable Customers, Users and other Services to access and view documents.</td><td>enable Customers and Users to view documents via various packages.

The measurement shall be calculated as the percentage of time within the operating hours that the Document View/Store service is Available, within the Service Period.

Document viewing service Availability =
(MP−SD)MP
x 100
where:
MP = total number of minutes within the relevant Service Period Operational Hours; and
SD = total number of minutes of Service Downtime in the relevant Service Period Operational Hours.
When calculating Document viewing service Availability in accordance with this KPI Document viewing service Operational Hours are set out in Schedule 2.1 (Services Description).</td><td>Minor KPI Failure</td><td><99.99% Availability</td><td>3</td></tr>
<tr><td></td><td></td><td></td><td>Serious KPI Failure</td><td><99.95% Availability</td><td>6</td></tr>
<tr><td></td><td></td><td></td><td>Severe KPI Failure</td><td><99.90% Availability</td><td>10</td></tr>
<tr><td></td><td></td><td></td><td>KPI Service Threshold</td><td><99.80% Availability</td><td>15</td></tr>
<tr><td colspan="2">Reporting and measurement</td><td></td><td colspan="3">Inclusions and exclusions</td></tr>
<tr><td colspan="2"><u>Frequency of measurement:</u>
Monthly</td><td></td><td colspan="3"></td></tr>
<tr><td>No</td><td>PI title and short description</td><td>PI Definition</td><td colspan="2">Severity levels</td><td>Service points</td></tr>
<tr><td>9.2</td><td><u>Performance:</u>
Documents View response performance.</td><td>The Document View Solution shall process 100% of all valid requests, from the point of receipt to the point its successfully provides the document(s) to the consuming system.</td><td>Target Performance Level</td><td>100% within 3000ms</td><td>0</td></tr>
<tr><td></td><td></td><td></td><td>Minor KPI Failure</td><td><100% within 3000ms</td><td>1</td></tr>
<tr><td></td><td></td><td></td><td>Serious KPI Failure</td><td><99.90% within 3000ms</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td>Severe KPI Failure</td><td><99.80% within 3000ms</td><td>3</td></tr>
</table>

			KPI Service Threshold	<99.70% within 3000ms	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
9.3	Availability: Contact Centre Servicing Solutions.	Where Customers will experience the systems utilised for call answering and responding, then the Supplier's "technical" Services must be Available as confirmed by automated testing means. The systems will include Contact Centre telephony system, IVR solution, call recording solution and any Solutions generating automated answers to Customers calling the Contact Centre. Each Supplier Solution shall be individually Available 99.99% of operating hours to allow Customers and Users to contact agents or automated voice solutions and complete their Jobs to be Done. At Service Commencement date, the following Solutions shall be provided: **OSCD1** None as Legacy Applications. **OSCD2** Case Management (ServiceNow). ECM – Alfresco. **OSCD3 onwards** Agent Portal (ServiceNow). NICE CXone (Omni Channel and WFM).	Target Performance Level	All Services 99.99% Availability	0
			Minor KPI Failure	One or more Services achieving <99.99% Availability	5
			Serious KPI Failure	One or more Services achieving <99.95% Availability	10
			Severe KPI Failure	One or more Services achieving <99.90% Availability	15
			KPI Service Threshold	One or more Services achieving <99.80% Availability	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly In any event the Service availability is tested sufficiently frequently to confirm the target levels of Availability are being met.					

	PolyAI. The measurement shall be calculated as the percentage of time within the operating hours that each Service is individually Available, within the Service Period. The automated test means shall run continuously to test each Service at a Test Frequency Interval of no greater than sixty (60) seconds. Each test run shall record and report the success or failure of that test. Where a test is failed, the Service shall be deemed to have been unavailable for that Test Frequency Interval. The Service Availability shall be calculated as: Service Availability = (MP−SD)MP*(MP−SD)MP* x 100 where: MP = total number of seconds within the relevant Service Period Operational Hours; and SD = total number of seconds of Service Downtime in the relevant Service Period Operational Hours. When calculating Availability in accordance with this KPI, the Operational Hours are set out in the Requirements in Schedule 2.1 (*Services Description*).	

No	KPI title and short description	KPI Definition	Severity levels		Service points
9.4	Availability: Customer Servicing Solutions.	Where Customers will directly experience the Supplier's "technical" Services, these Services must be Available as confirmed by automated testing means. Each Supplier Solution shall be Available 99.99% of operating hours to allow Customers and Users to access and complete their Jobs to be Done. At Service Commencement date, the following Solutions shall be provided: Secure Messaging - 24 x 7 Chat Bot – 24 x 7 Social Media Response Platform – 24 x 7 Co-Browsing - Contact Centre Hours - N.B The Co-Browsing element of this KPI will be held in abeyance pending formal approval of use of Co-Browsing by the Director and this aspect will be agreed in accordance with Clause 7.8. The measurement shall be calculated as the percentage of time within the operating hours that each Service is Available, within the Service Period. The automated test means shall run continuously to test each Service at a Test Frequency Interval of no greater than sixty (60) seconds. Each test run shall record and report the success or failure of that test. Where a test is failed, the Service shall be deemed to have been unavailable for that Test Frequency Interval.	Target Performance Level	All Services 99.99% Availability	0
			Minor KPI Failure	One (1) Service <99.99% Availability	3
			Serious KPI Failure	Two (2) Services <99.99% Availability, or; Any single Service <99.95% Availability	6
			Severe KPI Failure	Three (3) Services <99.99% Availability, or; Any single Service <99.90% Availability	10
			KPI Service Threshold	More than three (3) Services <99.99% Availability, or; Any single Service <99.80% Availability	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly In any event the Service availability is tested sufficiently frequently to confirm the target levels of Availability are being met.					

		The Service Availability shall be calculated as: Service Availability = (MP−SD)MP*(MP−SD)MP* x 100 where: MP = total number of seconds within the relevant Service Period Operational Hours; and SD = total number of seconds of Service Downtime in the relevant Service Period Operational Hours. When calculating Availability in accordance with this KPI 1, the Operational Hours are set out in Schedule 2.1 (*Services Description*).			
No	**PI title and short description**	**PI Definition**	**Severity levels**		**Service points**
9.5	Performance: Customer Servicing Solutions response performance.	The Customer Servicing Solutions (excluding Co-Browsing) process 100% of all valid User-initiated requests, or any responses to the User relating to a User-initiated request, from the point the Customer Servicing Solution receives it to the point its successfully responds to the consumer system, excluding the time the solution is waiting on a response from an agent or downstream system.	Target Performance Level	100% within 3000ms	0
			Minor KPI Failure	<100% within 3000ms	3
			Serious KPI Failure	<99.90% within 3000ms	6
			Severe KPI Failure	<99.80% within 3000ms	10
			KPI Service Threshold	<99.70% within 3000ms	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

No	PI title and short description	PI Definition	Severity levels		Service points
9.6	Performance: Co-Browsing Solution response performance.	The Co-Browsing Solution process 100% of all valid User-initiated requests, or any responses to the User relating to a User-initiated request, from the point the Customer Servicing Solution receives it to the point its successfully responds to the consumer system, excluding the time the solution is waiting on a response from an agent or downstream system.	Target Performance Level	100% within 500ms	0
			Minor KPI Failure	<100% within 500ms	3
			Serious KPI Failure	<99.90% within 500ms	6
			Severe KPI Failure	<99.80% within 500ms	10
			KPI Service Threshold	<99.70% within 500ms	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly			N.B This PI will be held in abeyance pending formal approval of use of Co-Browsing by the Director.		

KPI 10 – Patching					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
10.1	Critical Vulnerability Patches Deployed: All Critical Vulnerability Patches shall be Deployed within the specific timescales, within the Service Period.	Critical Vulnerability Patches Deployed shall be the total number of patches deployed in a Service Period, in accordance with the timescales set out in Schedule 2.4 (*Security Management*). The measurement will be calculated as the absolute number of Critical Vulnerability Patches that were Deployed outside of the timescales within the Service Period.	Target Performance Level	Zero (0) Critical Vulnerability Patches Deployed outside of the specified timescales	0
			Minor KPI Failure	One (1) Critical Vulnerability Patch Deployed outside of the specified timescales	5
			Serious KPI Failure	-	-
			Severe KPI Failure	-	-

			KPI Service Threshold	Two (2) or more Critical Vulnerability Patches Deployed outside of the specified timescales	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
10.2	High, Medium and Low Vulnerability Patches Deployed: All High, Medium and Low Vulnerability Patches shall be Deployed within the specific timescales, within the Service Period.	High, Medium and Low Vulnerability Patches Deployed shall be measured as the total number of patches deployed in a Service Period, in accordance with the timescales set out in Schedule 2.4 (*Security Management*). The measurement will be calculated as a percentage of the total number of High, Medium and Low Vulnerability Patches that have been successfully Deployed within the Service Period, in accordance with the following formula, rounded to two decimal places: Vulnerability Patches Deployed % = = (VI−VP)/ VI x 100 where: VI = total number of High, Medium and Low Vulnerabilities identified within the relevant Service Period; and VP = total number of High, Medium and Low Vulnerability Patches Deployed within the relevant Service Period.	Target Performance Level	98% of all High, Medium and Low Vulnerability Patches Deployed within the specified timescales	0
			Minor KPI Failure	<98% of all High, Medium and Low Vulnerability Patches Deployed within the specified timescales	3
			Serious KPI Failure	-	
			Severe KPI Failure	-	
			KPI Service Threshold	<90% of all High, Medium and Low Vulnerability Patches Deployed within the specified timescales	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

KPI 11 – Incident Management					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.1	P1 Initial Incident Resolution Time: All PI Incidents shall be Resolved within the specific timescales, within the Service Period.	All P1 Incidents shall be Resolved within the specified timescales in a Service Period. The measurement shall be calculated as the time taken from the identification and logging of a P1 Incident to the notification of restoration of Service or critical business service impacted as agreed with the Director, within the Service Period.	Target Performance Level	P1 95% of All Incidents Resolved within two (2) hours	0
			Minor KPI Failure	P1 <95% Incidents Resolved within two (2) hours	5
			Serious KPI Failure	P1 <95% Incidents Resolved within three (3) hours	12
			Severe KPI Failure	P1 <95% Incidents Resolved within four (4) hours	20
			KPI Service Threshold	P1 <95% Incidents Resolved within five (5) hours	30
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.2	P2 Initial Incident Resolution Time: All P2 Incidents shall be Resolved within the specific timescales, within the Service Period.	All P2 Incidents shall be Resolved within the specified timescales in a Service Period. The measurement shall be calculated as the time taken from the identification and logging of a P2 Incident to the notification of restoration of Service or critical business service impacted as agreed with the Director, within the Service Period.	Target Performance Level	P2 95% Incidents Resolved within four (4) hours	0
			Minor KPI Failure	P2 <95% Incidents Resolved within six (6) hours	3
			Serious KPI Failure	P2 <95% Incidents Resolved within eight (8) hours	6

			Severe KPI Failure	P2 <95% Incidents Resolved within twelve (12) hours	10
			KPI Service Threshold	P2 <95% Incidents Resolved within eighteen (18) hours	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.3	P3 Initial Incident Resolution Time: All P3 Incidents shall be Resolved within the specific timescales, within the Service Period.	All P3 Incidents shall be Resolved within the specified timescales in a Service Period. The measurement shall be calculated as the time taken from the identification and logging of a P3 Incident to the notification of restoration of Service or critical business service impacted as agreed with the Director, within the Service Period.	Target Performance Level	P3 90% Incidents Resolved within one (1) Working Day	0
			Minor KPI Failure	P3 <90% Incidents Resolved within one (1) Working Day	1
			Serious KPI Failure	P3 <90% Incidents Resolved within two (2) Working Days	2
			Severe KPI Failure	P3 <90% Incidents Resolved within four (4) Working Days	3
			KPI Service Threshold	P3 <90% Incidents Resolved within six (6) Working Days	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

No	KPI title and short description	KPI Definition	Severity levels		Service points
11.4	<u>P4 Initial Incident Resolution Time:</u> All P4 Incidents shall be Resolved within the specific timescales, within the Service Period.	All P4 Incidents shall be Resolved within the specified timescales in a Service Period. The measurement shall be calculated as the time taken from the identification of a P4 Incident to the notification of restoration of Service or critical business service impacted as agreed with NS&I, within the Service Period.	Target Performance Level	P4 100% Incidents Resolved within thirty (30) calendar days	0
			Minor KPI Failure	P4 <100% Incidents Resolved within thirty (30) calendar days	1
			Serious KPI Failure	P4 <100% Incidents Resolved within thirty-five (35) calendar days	2
			Severe KPI Failure	P4 <100% Incidents Resolved within forty (40) calendar days	3
			KPI Service Threshold	P4 <100% Incidents Resolved within forty-five (45) calendar days	4
Reporting and measurement			**Inclusions and exclusions**		
<u>Frequency of measurement:</u> Monthly					

No	KPI title and short description	KPI Definition	Severity levels		Service points
11.5	<u>P1 Incident Root Cause Analysis:</u> All PI Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period.	All PI Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period. The measurement shall be calculated as the percentage of Incidents with RCA completed within the specified timescales of an Incident being Resolved, within the Service Period.	Target Performance Level	95% of All P1 RCA produced within two (2) days	0
			Minor KPI Failure	<95% of all P1 RCA produced within two (2) days	3
			Serious KPI Failure	<95% of all P1 RCA produced within three (3) days	6
			Severe KPI Failure	<95% of all P1 RCA produced within four (4) days	10

			KPI Service Threshold	>5% of all P1 RCA produced after four (4) days	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.6	P2 Incident Root Cause Analysis: All P2 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period.	All P2 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period. The measurement shall be calculated as the percentage of Incidents with RCA completed within the specified timescales of an Incident being Resolved, within the Service Period.	Target Performance Level	95% of All P2 RCA produced within two (2) days	0
			Minor KPI Failure	<95% of all P2 RCA produced within two (2) days	3
			Serious KPI Failure	<95% of all P2 RCA produced within three (3) days	6
			Severe KPI Failure	<95% of all P2 RCA produced within four (4) days	10
			KPI Service Threshold	>5% of all P2 RCA produced after four (4) days	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.7	P3 Incident Root Cause Analysis: All P3 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period.	All Recurring P3 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period. "Recurring" for the purpose of this KPI shall mean two (2) or more of substantially the same Incident within three (3) consecutive months.	Target Performance Level	95% of All P3 RCA produced within five (5) days of the start of the following calendar month	0
			Minor KPI Failure	<95% of all P3 RCA produced within five (5) days of the start	1

		The measurement shall be calculated as the percentage of Incidents with RCA completed within the specified timescales of an Incident being Resolved, within the Service Period.		of the following calendar month	
			Serious KPI Failure	<95% of all P3 RCA produced within seven (7) days of the start of the following calendar month	2
			Severe KPI Failure	<95% of all P3 RCA produced within ten (10) days of the start of the following calendar month	3
			KPI Service Threshold	>5% of all P3 RCA produced after ten (10) days of the start of the following calendar month	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.8	P4 Incident Root Cause Analysis: All P4 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period.	All Recurring P4 Incidents shall have Root Cause Analysis completed within the specific timescales, within the Service Period. "Recurring" for the purpose of this KPI shall mean two (2) or more of substantially the same Incident within three (3) consecutive months. The measurement shall be calculated as the percentage of Incidents with RCA completed within the specified timescales of an Incident being Resolved, within the Service Period.	Target Performance Level	95% of All P4 RCA produced within five (5) days of the start of the following calendar month	0
			Minor KPI Failure	<95% of all P4 RCA produced within five (5) days of the start of the following calendar month	1
			Serious KPI Failure	<95% of all P4 RCA produced within ten (10) days of the start of the following calendar month	2

			Severe KPI Failure	<95% of all P4 RCA produced within fifteen (15) days of the start of the following calendar month	3
			KPI Service Threshold	>5% of all P4 RCA produced after fifteen (15) days of the start of the following calendar month	4
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.9	Permanent Fix Availability: All PI – P4 Incidents shall have a Permanent Fix Available within thirty (30) Working Days of the Incident being Resolved.	Where a fix has been identified as being required as a result of root cause analysis, all of those P1 – P4 Incidents shall have a permanent fix successfully made Ready for Deployment within thirty (30) Working Days of the Incident being Resolved. Ready for Deployment means that the Solution has been defined, tested in Unit/Component testing, and documented. The measurement shall be calculated as the percentage of Incidents with a Permanent Fix successfully being made Ready for Deployment within the specified timescales of an Incident being Resolved, within the Service Period. The thirty (30) Working Days target starts from the point at which the original incident was Resolved (i.e. the timescale runs in parallel with KPI 6 Incident Root Cause Analysis) Permanent Fix Ready for Deployment % =	Target Performance Level	100% within thirty (30) Working Days	0
			Minor KPI Failure	<100% within thirty (30) Working Days	3
			Serious KPI Failure	-	-
			Severe KPI Failure	-	-
			KPI Service Threshold	<90% within thirty (30) Working Days	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

		$\frac{(PF-NA)}{PF}$ x 100 where: PF = total number of Incidents with a Permanent Fix being successfully made Ready for Deployment within timescales within the relevant Service Period; and NA = total number of Incidents with a Permanent Fix not made Ready for Deployment within specified timescales within the relevant Service Period.			
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.10	Permanent Fix Deployment: All PI – P4 Incidents shall have a Permanent Fix Deployed within sixty (60) Working Days of the Incident being Resolved.	Where a fix has been identified as being required as a result of root cause analysis, all of those PI – P4 Incidents shall have a Permanent Fix successfully Deployed within sixty (60) Working Days of the Incident being Resolved. Deployment of the Permanent Fix means that the Solution defined under KPI 11.9 has been integration and/or regression tested and incorporated into the current production code set under an agreed change management process. The measurement shall be calculated as the percentage of Incidents with a Permanent Fix successfully Deployed within the specified timescales of an Incident being Resolved, within the Service Period. The sixty (60) Working Days target starts from the point at which the original Incident was Resolved. Permanent Fix Deployment % =	Target Performance Level	100% within sixty (60) Working Days	0
			Minor KPI Failure	<100% within sixty (60) Working Days	3
			Serious KPI Failure	-	-
			Severe KPI Failure	-	-
			KPI Service Threshold	<90% within sixty (60) Working Days	15
Reporting and measurement			**Inclusions and exclusions**		
Frequency of measurement: Monthly					

		$\frac{(PD-ND)}{PD}$ x 100 where: PD = total number of Incidents with a Permanent Fix being successfully Deployed within timescales within the relevant Service Period; and ND = total number of Incidents with a Permanent Fix not successfully Deployed within specified timescales within the relevant Service Period.			
No	**KPI title and short description**	**KPI Definition**	**Severity levels**		**Service points**
11.11	<u>Post Release Incident Rate:</u> No releases shall cause a P1 or P2 Incident in the live environment.	Zero P1 and P2 Incidents as a result of a new release into the live environment (within a period of ninety (90) calendar days).	Target Performance Level	100% of releases are deployed without P1 or P2 Incidents attributable to the release within ninety (90) calendar days of release date	0
			Minor KPI Failure	No P1 and one (1) P2	3
			Serious KPI Failure	One (1) P1 or two (2) P2	6
			Severe KPI Failure	Two (2) P1 or three (3) P2	12
			KPI Service Threshold	> Two (2) P1 or three (3) P2	15
Reporting and measurement			**Inclusions and exclusions**		
<u>Frequency of measurement:</u> Monthly					

<table>
<tr><th colspan="5">KPI 12 – Subsidiary Performance Indicators</th></tr>
<tr><th>No</th><th>PI title and short description</th><th>PI Definition</th><th colspan="2">Severity levels</th><th>Service Points</th></tr>
<tr><td rowspan="2">12.1</td><td rowspan="2">P1 Incident Communication Time.</td><td rowspan="4">The time taken for the Supplier to communicate a P1 Incident to the Director from identification/discovery and raise the appropriate Incident ticket (via the Incident Helpdesk). The communication should contain a number of elements – date occurred, date logged, systems/Services impacted, Supplier impacted, business areas impacted, Sustomer impact (numbers and products) where applicable.</td><td>Target Performance Level</td><td>99% within thirty (30) minutes M</td><td>0</td></tr>
<tr><td>PI Service Threshold</td><td><99% within thirty (30) minutes</td><td>15</td></tr>
<tr><td colspan="2">Reporting and measurement</td><td colspan="3">Inclusions and exclusions</td></tr>
<tr><td colspan="2"><u>Frequency of measurement:</u>
Monthly</td><td colspan="3"></td></tr>
<tr><th>No</th><th>PI title and short description</th><th>PI Definition</th><th colspan="2">Severity levels</th><th>Service Points</th></tr>
<tr><td rowspan="2">12.2</td><td rowspan="2">P2 Incident Communication Time.</td><td rowspan="4">The time taken for the Supplier to communicate a P2 Incident to the Director from identification/discovery and raise the appropriate Incident ticket (via the Incident Helpdesk). The communication should contain a number of elements – date occurred, date logged, systems/Services impacted, Supplier impacted, business areas impacted, Customer impact (numbers and products) where applicable.</td><td>Target Performance Level</td><td>99% within one (1) hour</td><td>0</td></tr>
<tr><td>PI Service Threshold</td><td><99% within one (1) hour</td><td>15</td></tr>
<tr><td colspan="2">Reporting and measurement</td><td colspan="3">Inclusions and exclusions</td></tr>
<tr><td colspan="2"><u>Frequency of measurement:</u>
Monthly</td><td colspan="3"></td></tr>
</table>

2. Definitions of Incident

P1	Critical	**P1 Incident** means an Incident which, in the reasonable opinion of the Director: (a) constitutes a loss or major disruption to one or more business critical Services; or (b) prevents Customers interacting or doing business with the Director; or (c) prevents Users from working or accessing the Supplier Systems; or (d) has a critical impact on the activities of the Director; or (e) causes significant financial loss and/or disruption to the Director; or (f) results in any material loss or corruption of Director Data; or (g) there is no workaround possible other than manual processes. **Non-exhaustive examples:** • An Incident which is in line or exceeds the Director's Risk Appetite for major or critical impact; • Incidents significantly affecting Customers' ability to contact the Contact Centre (e.g. complete failure of connectivity to the Contact Centre); • Loss of ability to access and view documents in the Document storage facility.
P2	Major	**P2 Incident** means an Incident which, in the reasonable opinion of the Director has the potential to: (a) Cause partial loss or intermittent disruption to one significant business system/service/process with low volumes; or (b) Cause partial loss or intermittent disruption to one significant business system/service/process where Customers and/or Users are affected; or (c) Cause partial loss or intermittent disruption to one or more non-critical business system/service/process; or (d) Have a major (but not critical) adverse impact on the activities of the Director and no workaround acceptable to the Director is available; or (e) Cause a financial loss and/or disruption to the Director or a Relevant Third Party Supplier which is more than trivial but less severe than the significant financial loss described in the definition of a P1 Incident. **Non-exhaustive examples:**

		• Support services are unavailable/affected which impact the KPI achievement in regards to the Director's Service Delivery Measures, Customer expectations or regulatory compliance; • Significant delays in Customers' requests being handled; or • Impact is in line or exceeds the Director's Risk Appetite for significant impact.
P3	Normal	**P3 Incident** means an Incident which, in the reasonable opinion of the Director has the potential to**:** (a) Cause partial loss or intermittent disruption to one or more non-critical business system/service/process which; (b) have a major adverse impact on the activities of the Director which can be reduced to a moderate adverse impact due to the availability of a workaround acceptable to the Director; or (c) have a moderate adverse impact on the activities of the Director. **Non-exhaustive examples:** • Does not directly impact Customers, but may impact low numbers (e.g. 5-10) of Users for non-critical activity; • Impacts in line or exceeds the Director's Risk Appetite for minor impact.
P4	Low	**P4 Incident** means an Incident which, in the reasonable opinion of the Director has the potential to: (a) cause partial loss or intermittent disruption to a single, non-critical systems/service/process that does not impact Customers and/or Users; or (b) have a minor adverse impact on the provision of the Services on third parties including a Relevant Third Party Supplier; or (c) an Incident comprising a flaw which is cosmetic and as such does not undermine any Customer and/or User's confidence in the information being displayed. **Non-exhaustive examples:** • Spelling error that does not directly impact the Customer experience or ability to make financial decisions on products; • Misalignment of data on screen display; or • Impact is in line or exceeds the Director's Risk Appetite for low impact.