Contract Reference Number: ICT 11098

Date: 31 March 2015

Agreement for the Supply of Software and Maintenance Services

between

TfL

and

Arqiva Limited

CONTENTS
Clause   **Page**

Schedules   83

THIS AGREEMENT is made on the date set out on the front page of this Agreement

BETWEEN

(1)   **Transport for London** (the **"Authority"**)

(2)   The party set out in **Schedule** 1 as being the Service Provider (the **"Service Provider"**)

BACKGROUND

(A)   The Authority wishes to procure and the Service Provider wishes to supply certain software and/or services, as set out below.

(B)   The parties have agreed to enter into this Agreement to define their contractual rights and liabilities in relation to such supply.

OPERATIVE PROVISIONS

DEFINITIONS

1.1   In this Agreement the following expressions shall have the following meanings unless inconsistent with the context:

"Acceptance"	date on which an Acceptance Certificate is issued
"Acceptance Certificate"	certificate issued by the Authority when the Software has been installed and implemented and has successfully passed the Acceptance Tests in accordance with **Schedule 6**
"Acceptance Criteria"	criteria referred to in **Schedule 6** for testing the Software (or relevant part thereof)
"Acceptance Tests"	tests that the party or parties, as set out in **Schedule 6**, will carry out using the test data and expected results, prepared by the party

	or parties as set out in **Schedule 6**, to determine whether the Software or any part of the Software complies with the Acceptance Criteria
"Additional Services"	services detailed in the **Annex** called **Additional Services** in **Schedule 2**, if any
"Agreed Equality Policy"	equality policy agreed between the Authority and the Service Provider as set out in **Schedule 9**, if any
"Agreement"	this Agreement, its Schedules, Annexes and Appendices (if any) and any other document expressly incorporated into this Agreement by virtue of any provision of this Agreement
"Agreement End Date"	date set out in **Schedule 1** as the Agreement End Date
"Authority Premises"	land or premises (including temporary buildings) owned or occupied by or on behalf of the Authority and/or any member of the TfL Group
"Authority Software"	software to be provided by the Service Provider to the Authority under this Agreement which is not Third Party Software or Service Provider Software, as may be updated, replaced or amended from time to time
a **"Business Day"**	a day other than a Saturday or Sunday or a public or bank holiday in England
"Business Hours"	hours set out in **Schedule 1**

"**Cessation Plan**"	a plan agreed between the parties or determined by the Authority pursuant to **Clause 25A** to give effect to a Declaration of Ineffectiveness
"**Change of Control**"	change of the control of a company, and "**control**" shall be as defined by Section 840 of the Income and Corporation Taxes Act 1988
"**Charges**"	charges set out in **Schedule 3**
"**Commencement Date**"	the date of this Agreement
"**Confidential Information**"	all information in respect of the business of the Authority and/or any of the TfL Group Members including, without prejudice to the generality of the foregoing, any ideas; business methods; pricing or financial information; business, financial, marketing, development or manpower plans; customer lists or details; computer systems and software; products or services including information concerning the Authority's and/or the TfL Group Members' relationships with actual or potential clients, customers or suppliers and the needs and requirements of the Authority and/or TfL Group Members and any other information which, if disclosed, will be liable to cause harm to the Authority and/or a TfL Group Member
"**Contract Information**"	(i) this Agreement in its entirety (including from time to time agreed changes to this Agreement) and (ii) data extracted from the invoices submitted pursuant to **clause 4**

	which shall consist of the Service Provider's name, the expenditure account code, the expenditure account code description, the document number, the clearing date and the invoice amount
"Copy"	individual copy on electromagnetic recording material of one or more of the programs constituting the Software
"Declaration of Ineffectiveness"	a declaration of ineffectiveness in relation to this Agreement made by a Court of competent jurisdiction pursuant to Regulation 47J of the Public Contracts Regulations 2006 or Regulation 45J the Utilities Contracts Regulations 2006
"Disaster"	unplanned interruption (whether of information processing facilities or systems or otherwise), including fire, interruption in power supply, act of terrorism, threat of act of terrorism, earthquake, extraordinary storm, flood or abnormal weather conditions, which impairs the ability of the Service Provider to perform the Services (in whole or in part and other than in some superficial manner) to the standard of the Service Levels and/or in accordance with this Agreement
"Disaster Recovery Plan"	Service Provider's plan for its emergency response, back-up procedures and business continuity in the event of a Disaster
"Dispute"	dispute or difference that may arise out of or

in relation to this Agreement

"Dispute Resolution Procedure"	procedure for resolving/attempting to resolve disputes, as set out in **clause 38**
"Documentation"	technical and user documentation (including report guides, user manuals, technical manuals, computer operation manuals, installation and support manuals, operating standards, specifications and training materials and the Specification) that describe in detail the configuration, installation, intended operation and maintenance of the Software (as applicable) as such written material may be updated from time to time in accordance with this Agreement
"DPA"	Data Protection Act 1998 and related secondary legislation
"Early Termination Charge"	the charge specified under **clause 24.2**.
"e-GIF"	UK Government's "e-government inter-operability framework" standard, as may be updated or replaced from time to time, details of which are available on the Cabinet Office website, www.govtalk.gov.uk
"Exit Plan"	plan for dealing with the exit of the Services upon termination or expiry, as agreed between the parties in writing and updated in accordance with **Schedule 10**
"Euro Compliant"	functioning and able to function accurately in any currency of the United Kingdom and the

	European Union, including any currency in use or currencies in concurrent use following partial or complete European Economic and Monetary Union
"FOI Legislation"	Freedom of Information Act 2000, all regulations made under it and the Environmental Information Regulations 2004, and any guidance issued by the Information Commissioner, the Ministry of Justice or the Department for Environment Food and Rural Affairs (including in each case its successors or assigns) in relation to such legislation
"Force Majeure Event"	any of the following: riot, civil unrest, war, act of terrorism, threat of act of terrorism, fire, earthquake, extraordinary storm, flood, abnormal weather conditions or other natural catastrophe or strikes, lock-outs or other industrial disputes (but excluding any strikes, lock-outs or other industrial disputes of or relating to employees of the party whose obligation to perform is thereby affected, or employees of such party's sub-contractors) to the extent that such event has materially affected the ability of the party relying on the Force Majeure Event (**"Affected Party"**) to perform its obligations in accordance with the terms of this Agreement but excluding any such event if those events should have been negated by implementation by the Service Provider of its' Disaster Recovery Plan or insofar as the event arises from or is

	attributable to the wilful act, omission or negligence of the Affected Party or the failure on the part of the Affected Party to take reasonable precautions to prevent such Force Majeure Event or its impact
"GLA"	the Greater London Authority
"Go Live"	means the date on which the Authority places the Software into live operation other than for testing purposes
"Holding Company"	company which from time to time directly or indirectly controls the Service Provider where **"control"** is as defined by section 840 of the Income and Corporation Taxes Act 1988
"Information"	information recorded in any form held by the Authority or by the Service Provider on behalf of the Authority
"Information Request"	request for any Information under the FOI Legislation
"Initial Tests"	tests that the Service Provider must carry out on the Software to determine whether it is in accordance with the Specification before the Software is submitted for Acceptance Tests in accordance with **Schedule 6**
"Insolvency Event"	any of the following:
	(a) the Service Provider and/or the Holding Company making any voluntary arrangement with its creditors or

becoming subject to an administration order;

(b) a receiver, administrative receiver, manager or administrator being appointed over all or part of the business of the Service Provider and/or the Holding Company;

(c) being a company, the Service Provider and/or the Holding Company having passed a resolution for its winding-up or being subject to a petition for its winding-up (except for the purposes of a voluntary amalgamation, reconstruction or other re-organisation without insolvency);

(d) the Service Provider and/or the Holding Company ceasing or threatening to cease to carry on its business for any reason and/or being unable to pay its debts within the meaning of the Insolvency Act 1986;

(e) being an individual or firm, the Service Provider becoming bankrupt or dying; or

(f) any similar event to those in (a) to (e) above occurring in relation to the Service Provider and/or the Holding Company under the law of any applicable jurisdiction

"Insurance" or   insurances, as set out in **Annex A** of

"Insurances"	Schedule 1
"Intellectual Property Rights" or "IPR"	any and all patents, trademarks, trade names, service marks, copyright, moral rights, rights in design, rights in databases, know-how, Confidential Information and all or any other intellectual or industrial property rights whether or not registered or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with all or any goodwill relating thereto
"Key Milestone Dates"	key dates for delivery of the Software, the Services, or parts thereof, as may be specified in the Project Plan
"Key Personnel"	Service Provider's key personnel set out in **Schedule 1**, as may be updated by agreement in writing from time to time
"Liquidated Damages Period"	period in which Liquidated Damages shall be paid, as set out in **Schedule 1**, if any
"Liquidated Damages"	financial damages as set out in **Schedule 1**, if any
"Losses"	all costs (including legal costs and costs of enforcement), expenses, liabilities (including any tax liability), injuries, direct, indirect or consequential loss (all three of which terms include pure economic loss, loss of profits, loss of business, depletion of goodwill and like loss), damages, claims, demands, proceedings and judgments

"Maintenance Services"	maintenance services for the Software as detailed in **Annex B** of **Schedule 2**, called **"Maintenance Services"**, if any
"Open Source"	Open Source Software means third party software code which is licensed upon terms which materially conform to either (i) the open source definition laid down by the body known as the Open Source Initiative or (ii) any generally accepted replacement for or alternative to such open source definitions
the **"parties"**	the parties to this Agreement
"Personal Data"	has the meaning given to it by section 1(1) of the Data Protection Act 1998
"Planned Change Freeze"	means the periods specified under the Project Plan (Schedule 5)
"Processing"	has the meaning given to it by section 1(1) of the Data Protection Act 1998 and **"Process"** and **"Processed"** will be construed accordingly
"Project Plan"	plan in relation to any part of the provision of the Software and/or Services as set out in **Schedule 5** or as agreed between the parties in writing from time to time
"Schedules"	schedules attached to and forming part of this Agreement
"Security Policy"	the TfL Group's security polic(y)(ies), the current version(s) of which is/are as set out

	in **Schedule 8**, as such security polic(y)(ies) may be updated by the Authority in writing from time to time
"Service Credits"	service credits as set out in the **Annexes** to **Schedule 2**, if any
"Service Level Period"	period in which Service Credits shall be paid, as set out in **Schedule 2**, if any
"Service Levels"	standards of performance to be achieved for the Services as set out in **Schedule 2**, if any
"Service Provider Software"	Software where the IPR is to be retained by the Service Provider, as agreed between the parties, as set out in **Schedule 1**, as such software may be updated, replaced or amended from time to time, if any
"Service Provider's Equipment"	equipment and materials of whatsoever nature used by the Service Provider in providing the Services which do not themselves form part of the Services or the Software and in which title is not intended to pass to the Authority under this Agreement, as set out in **Schedule 1**, if any
"SAFE Software Sub-Licence"	means the SAFE Software Licence terms and conditions as set out in Schedule 11, in respect of the Third Party Software to be supplied by the Service Provider
"Service Provider's IPR"	parts of the Software or Services which exist prior to the commencement of this Agreement which are owned by the Service Provider and the Intellectual Property Rights

in which are to be retained by the Service Provider, as specified in **Schedule 1**, if any

"Service Provider's Personnel"	employees, officers, suppliers, sub-contractors and agents of the Service Provider engaged in the performance of any of the Services and including the Key Personnel
"Services"	services required from the Service Provider in building and supplying the Software; the Maintenance Services, if any; and the Additional Services, if any, in each case as are specified in **Schedule 2** (including its **Annexes**), together with any services, functions and responsibilities (including any incidental services, functions and responsibilities) not specifically set out in this Agreement but which are within the scope of the Services and which are reasonably to be inferred from this Agreement; and any other services from time to time agreed between the parties in writing to be supplied by the Service Provider to the Authority under this Agreement
"Site(s)"	Authority Premises, as specified in **Schedule 1**
"Software"	Service Provider Software, the Authority Software, and the Third Party Software
"Specification"	either the TfL Group's Statement of Requirements or the TfL Group's written specification for the Software, as set out in

	Schedule 4, which may be updated by agreement in writing from time to time by both parties and where a full Specification has not yet been agreed between the parties, any **"Specification"** shall mean the TfL Group's Statement of Requirements until such time that the full agreed Specification has been signed off between the parties in writing after which point **"Specification"** shall be deemed to refer to such fully agreed specification
"Statement of Requirements"	high level Statement of Requirements of the Authority for the Software, as set out in **Schedule 4**, if applicable, as may be updated or superseded by a full specification in writing from time to time
"Successor Authority"	person created by statute or subordinate legislation to assume all (or part of) the TfL Group's functions
"TfL"	Transport for London, a statutory corporation whose principal place of business is at Windsor House, 50 Victoria Street, London SW1H 0TL
"TfL Group"	the Authority and the other companies or organisations related to TfL, as set out in **Schedule 1**
"TfL Group Member"	any member of the TfL Group
"TfL Group's Liability Cap"	amounts set out in **Schedule 1**

"Third Party"	person, partnership, company or any other undertaking not being the Service Provider or a TfL Group Member
"Third Party IPR"	all parts of the Software and Services which are owned by a third party, the Intellectual Property Rights in which are to be retained by that third party EXCEPT for the parts of the Software and Services set out in Schedule 1, which are expressly agreed to transfer to the Authority (such list as may be updated, replaced or amended from time to time)
"Third Party Software"	third party software to be provided to the Authority under this Agreement which is specified as Third Party Software in **Schedule 1**, as may be updated, replaced or amended from time to time
"Transparency Commitment"	the transparency commitment stipulated by the UK government in May 2010 (including any subsequent legislation) in accordance with which the Authority is committed to publishing its contracts, tender documents and data from invoices received
"Virus"	program code or set of instructions intentionally or recklessly constructed with the ability to damage, interfere with or otherwise adversely affect computer programs, data files or operations including trojan horses, logic bombs, time bombs, data disabling code or any similar materials of

any nature

"Warranty Period" warranty period(s) set out in **Schedule 1**

1.2 a reference to the singular includes the plural and vice versa, and a reference to any gender includes all genders;

1.3 a reference to any statute, enactment, order, regulation or other similar instrument, unless the context otherwise requires, shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended or re-enacted (whether in whole or in part) by any subsequent statute, enactment, order, regulation or instrument and shall include all statutory instruments or orders made pursuant to it whether in place before or after the date of this Agreement;

1.4 except as specified in **clause 1.3** or expressly elsewhere in this Agreement, a reference to any document shall be construed as a reference to the document as at the date of execution of this Agreement;

1.5 headings are included in this Agreement for ease of reference only and do not affect the interpretation or construction of this Agreement;

1.6 references to clauses, Schedules, Annexes and Appendices are, unless otherwise provided, references to clauses of and Schedules, Annexes and Appendices to this Agreement and any reference to a paragraph in any Schedule or Annex or Appendix (if any) shall, in the absence of provision to the contrary, relate to the paragraph in that Schedule or Annex or Appendix;

1.7 in the event, and only to the extent, of any conflict between the clauses, the Schedules, the Annexes, and the Appendices (if any), the clauses prevail, except where:

1.7.1 the conflicting part of the Schedule, Annex or Appendix is explicitly expressed to take precedence; or

1.7.2 the conflict is with a provision in **Annex B** of **Schedule 1** (Special Conditions of Contract), in which case the provisions in **Annex B** of **Schedule 1** shall prevail;

1.8 the Schedules, Annexes and Appendices (if any) form part of this Agreement and, subject to **clause 1.7**, will have the same force and effect as if expressly set out in the body of this Agreement;

1.9 the expression **"person"** means any individual, firm, body corporate, unincorporated association, partnership, government, state or agency of a state or joint venture; and

1.10 the words "including", "includes" and "included" will be construed without limitation unless inconsistent with the context.

2. **COMMENCEMENT AND DURATION**

2.1 This Agreement shall commence on the Commencement Date and shall, unless and until terminated in accordance with its terms, continue in force until the earlier of:

2.1.1 the completion of the Services; or

2.1.2 the Agreement End Date,

(being the **"Term"**).

3. **SERVICE PROVIDER'S OBLIGATIONS**

3.1 The Service Provider shall supply the Software and perform the Services in accordance with the terms and conditions of this Agreement.

3.2 The Service Provider shall perform its obligations in relation to the Acceptance Tests in accordance with **Schedule 6**.

3.3 The Service Provider:

3.3.1 acknowledges that it has sufficient information about the TfL Group and its requirements for the Software and/or the Services and that it has made all appropriate and necessary enquiries to enable it to supply the Software and perform the Services in accordance with this Agreement;

3.3.2 shall neither be entitled to any additional payment nor excused from any obligation or liability under this Agreement due to any

misinterpretation or misunderstanding by the Service Provider of any fact relating to the TfL Group's requirements for the Software and/or the Services or otherwise;

3.3.3 shall comply with all lawful and reasonable directions of the Authority relating to its supply of the Software and performance of the Services;

3.3.4 shall, when required, give to the Authority such written or oral advice or information regarding the Software and/or the Services as the Authority may reasonably require;

3.3.5 where a format for electronic receipt of orders by the Service Provider is set out in **Schedule 1**, shall, unless the Authority requires otherwise, receive orders in such format and shall maintain its systems to ensure that it is able to do so throughout the Term; and

3.3.6 shall provide training to the Authority's personnel (including its employees, officers, suppliers, sub-contractors and agents) as specified in **Schedule 2**.

3.4 Notwithstanding anything to the contrary in this Agreement, the TfL Group's discretion in carrying out its statutory duties shall not be fettered or otherwise constrained or affected by any provision of this Agreement.

3.5 The Service Provider shall provide the Service Provider's Personnel as necessary for the proper and timely performance and management of the Services in accordance with the Agreement and shall give the Authority, if so requested, full particulars of all such persons who are or may be at any time employed on performing the Agreement. The Service Provider shall ensure that all Service Provider's Personnel deployed on work relating to the Agreement shall be properly managed and supervised.

3.6 Subject to the provisions of this **clause 3**, the Service Provider shall maintain the continued involvement of the Key Personnel in the performance of the Services and shall take all reasonable steps to avoid changes to any of its staff designated as Key Personnel. The Service Provider shall give the

Authority reasonable notice of any proposals to change Key Personnel and **clause 3.11** shall apply to the proposed replacement personnel.

3.7 The Service Provider will only use personnel to perform the Services who:

3.7.1 are suitably qualified and experienced to perform their role in performing the Services;

3.7.2 hold up to date and comply with professional certifications and qualifications relevant to the Services they are providing; and

3.7.3 in these and any other respects are acceptable to the Authority.

The Supplier shall demonstrate compliance with this **clause 3.7** as required by the Authority from time to time.

3.8 Without prejudice to any of the Authority's other rights, powers or remedies (including under **clause 3.7**), the Authority may (without liability to the Service Provider) deny access to such Service Provider's Personnel to any Authority Premises if such Service Provider's Personnel in the Authority's view have not been properly trained in any way required by this Agreement and/or are otherwise incompetent, negligent, and/or guilty of misconduct and/or who could be a danger to any person and shall notify the Service Provider of such denial in writing and in which case the Service Provider shall immediately remove such Service Provider's Personnel from performing the Services and provide a suitable replacement (with the Authority's prior written consent in the case of Key Personnel).

3.9 If the Authority requests, for bona fide reasons, that any member of the Service Provider's Personnel should cease to be involved in the supply of the Software or the performance of the Services under this Agreement, it shall notify the Service Provider in writing and state the reasons for the request. If the Service Provider agrees to the request (such agreement not to be unreasonably withheld) the said member shall be removed immediately and the Service Provider shall provide a suitably and similarly qualified replacement as soon as reasonably practicable and, in any event, within five (5) Business Days unless otherwise agreed. The removal of a member of the Service Provider's Personnel will not relieve the Service Provider from

performance of its obligations under this Agreement nor provide grounds for an extension of time for the supply of the Software or the performance of the Services.

3.10 The Service Provider shall not (except where the individuals are clearly not required for the performance of that part of the relevant Services) assign any of the Key Personnel to other duties which would prevent them from or interfere with their ability to properly carry out their duties in respect of the Services without the prior consent of the Authority. This shall not prevent the Service Provider from allowing members of the Service Provider's Personnel to take sickness, maternity, paternity, compassionate, religious or holiday leave or to attend a reasonable number of training courses.

3.11 In the event that a member of the Key Personnel resigns or shall for any reason cease to be engaged in the provision of the Services, the Service Provider shall ensure that a suitably and similarly qualified replacement who is acceptable to the Authority is appointed as soon as reasonably practicable and, in any event, within five (5) Business Days unless otherwise agreed; that there is a reasonable hand-over period (and that the costs of bringing the replacement up to the required level of knowledge are borne by the Service Provider); and that the performance of the Services are not affected. The Authority shall not unreasonably withhold agreement to the appointment of such replacement.

3.12 The Service Provider acknowledges and agrees that it shall be wholly responsible for the acts and omissions of the Service Provider's Personnel regardless of whether or not they are employees of the Service Provider. The Authority shall be wholly responsible for the acts or omissions of its personnel and any other person, entity or agent acting on its behalf (other than the Service Provider).

3.13 The parties shall each comply with their respective obligations set out in **Schedule 10**. Within sixty (60) days of the Commencement Date, the parties shall agree an Exit Plan in accordance with the provisions of **Schedule 10**.

4. **CHARGES AND PAYMENTS**

4.1   Subject to the Service Provider complying with and performing properly its obligations under this Agreement, the Service Provider shall be entitled to invoice the Authority in accordance with this **clause 4**.

4.2   In consideration of the proper performance of the Services and the supply of the Software in accordance with this Agreement, the Service Provider may invoice the Authority the Charges in respect of the Software and the Services at the amounts and on the basis set out in **Schedule 3**. Where no invoicing dates are set out in **Schedule 3**, then the Service Provider shall be entitled, within thirty (30) days following the end of each calendar month, or upon a milestone payment date set out in any Project Plan (as applicable), to submit an invoice in respect of the Charges arising during such month or upon achievement of such milestone (as applicable). For the avoidance of doubt, the Service Provider may not invoice the Authority for payments in relation to Key Milestone Dates or any other agreed payment milestones until such time that the Service Provider has delivered the applicable Services and/or parts of the Software and has fully performed its obligations in relation to such Key Milestone Dates or other agreed payment milestones.

4.3   Any sum payable by one party to the other under this Agreement will be exclusive of Value Added Tax (**"VAT"**) and any other similar tax which may be chargeable and which will be payable in addition to the sum in question at the rate for the time being prescribed by law on delivery of a valid VAT invoice.

4.4   The Service Provider shall submit invoices to the postal address stated in **Schedule 1** (or as otherwise specified by the Authority from time to time) or, where an electronic format for submission of invoices is set out in **Schedule 1**, such electronic format shall, unless the Authority requires otherwise, be used. Each such invoice shall contain all information required by the Authority including the Contract Reference Number, SAP order number, the Service Provider's name and address, a separate calculation of VAT and an adequate description of the Services provided.

4.5 If the Authority considers (acting reasonably) that any sums, fees or other charges claimed by the Service Provider in any invoice have been correctly calculated and that such invoice is correct, the invoice shall be approved and payment shall be made by bank transfer (Bank Automated Clearance System (**"BACS"**)) or such other method as the Authority may choose from time to time within thirty (30) days of receipt of such invoice, or within such other time period as may be agreed under **Schedule 1**.

4.6 No payment made by the Authority (including any final payment) or act or omission or approval by the Authority (whether related to payment or otherwise) shall:

4.6.1 indicate or be taken to indicate the TfL Group's acceptance or approval of the Services or Software or any part of them or any act or omission of the Service Provider, or otherwise prejudice any rights, powers or remedies which the Authority may have against the Service Provider, or absolve the Service Provider from any obligation or liability imposed on the Service Provider under or by virtue of this Agreement; or

4.6.2 prevent the Authority from recovering any amount overpaid or wrongfully paid including payments made to the Service Provider by mistake of law or fact. Without prejudice to **clause 4.8**, the Authority shall be entitled to withhold such amount from any sums due or which may become due to the Service Provider or the Authority may recover such amount as a debt.

4.7 In the event that the United Kingdom joins the European Economic and Monetary Union, the Authority shall require the Service Provider, at no additional charge, to convert any sums payable in connection with this Agreement from sterling to Euros in accordance with EC Regulation Number 1103/97.

4.8 All damages, costs, charges, expenses, debts, sums or other amounts owing (contingently or otherwise) to or incurred by the Authority arising out of or attributable to this Agreement or any other contract between the Authority or

any TfL Group Member and the Service Provider (howsoever arising and whether any such liability is present or future, liquidated or unliquidated and irrespective of the currency) may be deducted by the Authority from monies due or which may become due to the Service Provider under this Agreement or the Authority may recover such amount as a debt. The TfL Group's rights under this **clause 4.8** will be without prejudice to any other rights or remedies available to the Authority under this Agreement or otherwise.

4.9   If the Authority receives an invoice which the Authority reasonably believes specifies a Charge which is not valid or properly due or in respect of which any Service has not been duly and properly provided or where the Authority reasonably believes the invoice has not been calculated correctly or if the invoice contains any other error or inadequacy (**"Disputed Charge"**):

    4.9.1   the Authority shall pay to the Service Provider the part of the Charges under that invoice which is not a Disputed Charge;

    4.9.2   the Authority may withhold payment of the Disputed Charge in that invoice and, in that case, the Authority shall promptly (and in any event within thirty (30) days after receipt of the invoice) notify the Service Provider of the nature of the dispute and the parties shall commence, within five (5) days after the receipt of the TfL Group's notice, to resolve the dispute in accordance with the dispute resolution procedure set out in **clause 38**; and

    4.9.3   once the dispute has been resolved, the Authority shall pay any amount due as part of that resolution within ten (10) days of such resolution.

4.10   Except where otherwise provided in this Agreement, the Charges shall be inclusive of all costs of staff, facilities, equipment, materials and other expenses whatsoever incurred by the Service Provider in discharging its obligations under this Agreement.

4.11   Interest shall accrue at the interest rate of two percent (2%) above the base rate of HSBC Bank plc from time to time on all sums due and payable under this Agreement from the due date until the date of actual payment (both

before and after judgement). All such interest shall be calculated on the basis of the actual number of days elapsed, over a three hundred and sixty five (365) day year and compounded at monthly intervals. The parties agree that this provision constitutes a substantial remedy for late payment of any sum payable under this Agreement in accordance with s8(2) of the Late Payment of Commercial Debts (Interest) Act 1998.

5.   **SOURCE CODE, ESCROW AND VERIFICATION SERVICES**

5.1   The source code to any Software in which the Intellectual Property Rights are, or are to be, owned by the Authority, together with any programmers' notes and other documentation reasonably required to operate the source code in object code form and to maintain and adapt the source code, shall be supplied to the Authority when that part of the Software is supplied to the Authority (**"the Authority Materials"**).

5.2   The source code to any Software forming part of the Service Provider's IPR and/or Third Party IPR, together with any programmers' notes and other documentation reasonably required to operate the source code in object code form and to maintain and adapt the source code (**"Escrow Materials"**) shall, where requested by the Authority in **Schedule 1**, be subject to source code deposit arrangements and verification services to be entered into, on such terms as are reasonably acceptable to the Authority, within thirty (30) days of the TfL Group's request to do so (whether in relation to part or all of the Software) for the benefit of the TfL Group and its authorised agents with either NCC International Limited (**"NCC"**) (on NCC's then standard terms) or any other reputable escrow agent agreed to by the Authority and providing for the release of the source code of such Software in the event of insolvency (or analogous events) of the Service Provider, inadequate performance of support or maintenance obligations (if any) or cessation of trade by the Service Provider.

5.3   Where requested by the Authority, the Service Provider shall procure that NCC (or such other escrow agent as the Authority considers appropriate) enters into the escrow/verification agreement. The charges payable to NCC

or other escrow agent shall be borne by the Authority, unless set out otherwise in **Schedule 1**.

5.4 The Service Provider shall at all times ensure that the Escrow Materials deposited with NCC or other escrow agent are capable of being used to generate and maintain and adapt the latest version of the Software and the Service Provider shall deliver to NCC or other escrow agent an updated copy of the Escrow Materials as and when necessary for this purpose or when requested to do so by the Authority.

5.5 This **clause 5**4.11 shall survive termination of this or part of this Agreement.

6. **THE TFL GROUP'S OBLIGATIONS**

6.1 The Authority shall:

6.1.1 purchase the Software and the Services in accordance with the terms of this Agreement;

6.1.2 subject to **clauses 4.8** and **4.9**, pay all sums, fees and other charges due under this Agreement upon the dates provided for under this Agreement;

6.1.3 allow the Service Provider access to Sites in accordance with **clause 11**;

6.1.4 provide the Service Provider, on request and within a reasonable period thereafter, with information and assistance that the Service Provider may reasonably require.

6.1.5 comply with the terms set out in the SAFE Software Sub-Licence.

7. **DOCUMENTATION**

7.1 All Documentation prepared by the Service Provider pursuant to this Agreement shall, unless otherwise agreed by the parties, meet the following minimum requirements:

7.1.1 it and all referenced portions of other documents shall be clearly and concisely written; and

7.1.2 where applicable, it shall specify and describe the policy, specification or other subject matter in sufficient detail and in an easy to follow manner, so as to enable the TfL Group's staff or contractors trained and skilled to the level fairly expected of a person in the relevant position, to make full and efficient use of the Documentation for the purposes for which it was requested and/or written; and

7.1.3 it shall not refer to any document not provided to or already in the possession of the Authority; and

7.1.4 unless the Authority requests that such Documentation be subject to the Acceptance Tests, it shall be submitted to the Authority for approval and be subject to approval by the Authority in accordance with **clause 7.2**.

7.2 The Documentation to be submitted to the Authority for approval in accordance with **clause 7.1** shall be subject to one (1) draft correction cycle as specified in this **clause 7.2**. Unless agreed otherwise, the Authority shall, within five (5) days of the Service Provider submitting the Documentation either notify the Service Provider in writing of its approval of the Documentation (as applicable) or provide the Service Provider with its reasons in writing why such item(s) (or any part of it) is not approved whereupon the Service Provider shall make the required amendments and re-submit the revised Documentation to the Authority and the foregoing provisions shall apply. If the revised Documentation is not approved by the Authority and/or if the Service Provider does not accept the TfL Group's reasoning in relation to such non-approval, representatives of the parties will use their respective reasonable endeavours to resolve, in good faith, such non-approval/non-acceptance (as applicable) within thirty (30) days of the Authority submitting its reasons for such non-approval or (if later) the Service Provider's notification of non-acceptance of the TfL Group's reasons for non-approval (whichever is applicable). If, following the expiration of such

period, the Documentation has not been approved by the Authority, the matter shall be referred for resolution in accordance with **clause 38**.

8. **PERFORMANCE AND DELAY**

8.1 In respect of each of the Services to be performed under this Agreement, the Service Provider shall provide or complete the performance of such Service(s) on or before the applicable date specified in the applicable Project Plan or, in the event no such date is specified, promptly having regard to the nature of the project (**"Milestone"**). Time for the supply of the Software and provision of the Services shall be of the essence of this Agreement.

8.2 The Service Provider shall notify the Authority in writing as soon as reasonably practicable after becoming aware of any actual or likely failure to comply with any Milestone. Such written notice shall contain a detailed explanation of the causes of, and responsibility for, the delay, details of actions taken and to be taken by the Service Provider (and, to the extent that the Service Provider considers that the Authority is responsible for such delay, actions it requests be taken by the Authority) to remedy such delay and any effects such delay may have on the performance of the Services or supply of the Software and on the ability to meet the next Milestone or any other applicable Milestone. Without prejudice to any liability of either party, both parties shall use their reasonable endeavours to overcome and/or mitigate any such actual or anticipated delay.

8.3 If the Service Provider shall fail (to the extent that such failure was not directly due to any failure by the Authority to comply with its obligations under this Agreement) to provide the Service(s) or supply the Software in accordance with this Agreement by the Milestone then notwithstanding anything else contained in this Agreement the Service Provider shall not be entitled to any payment for any additional time spent and materials used by the Service Provider in providing the Service(s).

8.4 The Service Provider shall deliver the applicable parts of the Software and Services on or before the Key Milestone Dates. Save where such failure is caused by any omission by the Authority, the Authority shall be entitled to

Liquidated Damages, if applicable, in relation to any failure by the Service Provider to meet such Key Milestone Dates. The parties agree that such Liquidated Damages are a genuine and reasonable pre-estimate of the loss which the Authority would suffer during the Liquidated Damages Period arising from a failure by the Service Provider to provide the Software and/or Services (or parts thereof) as contemplated in this **clause 8.4**. The Liquidated Damages shall be the TfL Group's only financial remedy for failure to meet the Key Milestone Dates during the Liquidated Damages Period unless the Service Provider has failed to provide the undelivered parts of the Software and/or Services it has previously failed to provide by the end of the Liquidated Damages Period in which case the Authority shall be entitled to bring a claim for further damages in respect of financial losses suffered during and after such Liquidated Damages Period. The provisions of this **clause 8.4** shall be without prejudice to the TfL Group's other rights and remedies under this Agreement, including the TfL Group's rights to seek injunctive relief in any court of competent jurisdiction and/or to claim damages.

8.5 Where Service Levels and/or Service Credits are set out in **Schedule 2**, the Service Provider agrees that the Services shall comply in all respects with the Service Levels, and the Authority shall be entitled to the Service Credits in relation to any failure by the Service Provider to meet such Service Levels. Save where such failure is caused by any omission by the Authority, the parties agree that such Service Credits are a genuine and reasonable pre-estimate of the loss which the Authority would suffer during the Service Level Period arising from a failure by the Service Provider to provide the Services as contemplated in this **clause 8.5**. The provisions of this **clause 8.5** shall be without prejudice to the TfL Group's other rights and remedies under this Agreement, including the TfL Group's rights to seek injunctive relief in any court of competent jurisdiction and/or to claim damages where the loss suffered exceeds the Service Credits.

9. **WARRANTIES AND OBLIGATIONS**

9.1 Without prejudice to any other warranties expressed elsewhere in this Agreement or implied by law, the Service Provider warrants, represents and undertakes to the TfL Group that:

9.1.1 the Service Provider:

has full capacity and authority and all necessary licences, permits, permissions, powers and consents (including, where its' procedures so require, the consent of its Holding Company), if any, to enter into and to perform this Agreement; and

is aware of the purposes for which the Services and the Software are required and acknowledges that the TfL Group is reliant upon the Service Provider's expertise and knowledge in the supply of the Software and the provision of the Services; and

is entering into this Agreement as principal and not as agent for any person and that it will act as an independent contractor in carrying out its obligations under this Agreement;

9.1.2 this Agreement is executed by a duly authorised representative of the Service Provider;

9.1.3 all materials, equipment and goods recommended, used or supplied by the Service Provider in connection with this Agreement shall be of satisfactory quality within the meaning of the Sale of Goods Act 1979, sound in design, fit for purpose, shall comply with all statutory requirements and regulations relating to their sale and use and shall be in conformance in all respects with the requirements of the TfL Group including the Specification;

9.1.4 the Service Provider shall provide the Services:

with the high degree of skill, care and diligence normally exercised by recognised professional firms or by highly skilled and

experienced companies providing services of a similar scope, type and complexity to the Services with sufficient resources including project management resources;

in conformance in all respects with the requirements of the Authority and so that they fulfil the purpose indicated by or to be reasonably inferred from such requirements;

in a safe manner and free from any unreasonable or avoidable risk to any person's health and well-being and in an economic and efficient manner;

so that they are properly managed and monitored and shall immediately inform the Authority if any aspect of the Agreement is not being or is unable to be performed;

9.1.5 each part of the Software will, on the date on which it is supplied in accordance with this Agreement and for the Warranty Period thereafter, fulfil the TfL Group's requirements and comply with the Specification, and that if any part of the Software materially fails to comply in accordance with this **clause 9.1.5** at any time during the Warranty Period the Service Provider shall comply with **clause 9.3**;

9.1.6 without prejudice to **clause 9.1.5**, the Software (whether supplied or recommended for purchase by the TfL Group in connection with this Agreement) will be fully compatible with the TfL Group's computer and system infrastructures (including its' operating environment) set out in any Invitation to Tender (as may be superseded by the Specification) or notified to the Service Provider in writing from time to time;

9.1.7 the Service Provider shall fully co-operate with the TfL Group's agents, representatives or contractors (including other suppliers of computing products and services) and supply them with such

information, materials and assistance as the Authority may reasonably request or authorise from time to time;

9.1.8 all of the Service Provider's liabilities, responsibilities, and obligations shall be fulfilled in compliance with all applicable laws, enactments, orders, regulations, codes of practice, licences, waivers, consents, registrations, approvals, and other authorisations of competent authorities (**"Applicable Laws"**) and that the TfL Group's possession and/or use of the Software and/or its receipt of the benefit of the Services will not place the Service Provider or any of those persons so named in this clause in breach of any Applicable Law(s), provided that the Service Provider shall have no liability under this clause in respect of any breach of such Applicable Law(s) to the extent such breach is caused by the negligent, wilful or fraudulent act and/or omission of the Authority. The Change Control Provisions shall apply in the event that a change in law requires changes to the Software to be implemented by the Service Provider where the changes are peculiar to the business of the Authority or the TfL Group;

9.1.9 the Service Provider shall:

not introduce into any of the TfL Group's computer systems anything, including any computer program code, Virus, authorisation key, licence control utility or software lock, which is intended by any person to, is likely to, or may:

impair the operation of the Software or any other computer systems or programs in the possession of the TfL Group or impair the receipt of the benefit of the Service(s); or

cause loss of, or corruption or damage to, any program or data held on the TfL Group's computer systems,

and this **clause 9.1.9** shall apply notwithstanding that any such things are purported to be used for the purposes of protecting the

Service Provider's IPR, Third Party IPR, the Service Provider's contractual rights or other rights; or

not damage the reputation of the TfL Group;

9.1.10   the media on which any Software is supplied will be free from material defects in materials and workmanship under normal use;

9.1.11   it shall not and shall ensure that its Personnel and subcontractor's do not, without the TfL Group's prior written consent (such consent to be signed off by an authorised signatory of the Authority), include in the Software any third party software code which materially conforms to either (a) the then current Open Source definition laid down by the Open Source Initiative; or (b) any generally accepted replacement for or alternative to such Open Source definition at the relevant time;

9.1.12   the Service Provider shall ensure that the Software and any software, electronic or magnetic media, hardware or computer system recommended by the Service Provider for use in connection with this Agreement shall:

where specified by the Authority in **Schedule 1**, be Euro Compliant;

not have its functionality or performance affected, or be made inoperable or be more difficult to use by reason of any data related input or processing in or on any part of such software, electronic or magnetic media, hardware or computer system;

not cause any damage to, loss of or erosion to or interfere adversely or in any way with the compilation, content or structure of any data, database, software or other electronic or magnetic media, hardware or computer system used by, for or on behalf of any the TfL Group Member and/or any third party, on which it is used or with which it interfaces or comes into contact; and

be compliant with e-GIF,

and any variations, enhancements or actions undertaken by the Service Provider in respect of such software, electronic or magnetic media, hardware or computer system shall not affect the Service Provider's compliance with this **clause 9.1.12**.

Subject to **clause 9.1.8**, in all cases the costs of compliance with this **clause 9.1** shall be borne by the Service Provider.

9.2   The Service Provider shall ensure that the benefit of any and all warranties which it receives in respect of any Third Party Software are passed on to the TfL Group such that the TfL Group can enforce those warranties directly against such Third Party Software licensors.

9.3   Without prejudice to any other rights, powers or remedies the Authority may have, in the event of any breach(es) of the warranties set out at **clauses 9.1.3**, **9.1.4**, **9.1.5**, **9.1.6**, **9.1.8**, **9.1.9**, **9.1.10, 9.1.11** and **9.1.12** the Service Provider shall promptly (and, if applicable, in accordance with any relevant Service Level) supply such services as are necessary to remedy such breach(es) and to prevent the re-occurrence of such breach(es) in the future. To the extent that any such breach(es) re-occurs (notwithstanding, in relation to the limited warranty contemplated in **clause 9.1.5**, the fact that the relevant Warranty Period may have ended) then, subject to the cause of the said re-occurrence being the same or similar to that which caused the initial breach(es), the Service Provider shall forthwith supply such further Services as are necessary to remedy such breach(es) and to prevent any further re-occurrence thereof. Any Services required to be performed pursuant to this **clause 9.3** shall be performed at no additional cost to the Authority.

9.4   Each warranty and obligation in this **clause 9** shall be construed as a separate warranty or obligation (as the case may be) and shall not be limited or restricted by reference to, or reference from, the terms of any other such warranty or obligation or any other term of this Agreement.

10.   **CONFLICT OF INTEREST**

10.1 The Service Provider warrants that it does not have an interest in any matter where there is or is likely to be a conflict of interest with the Agreement or any member of the TfL Group and that (except as provided below) it shall not act for any person, organisation or company where there is or is likely to be such a conflict of interest. This clause shall not prevent the Service Provider from providing services to an existing client of the Service Provider to whom the Service Provider is, as at the date of this Agreement, providing services provided that the Service Provider shall:

10.1.1 not act for any such client in respect of any transactions between any member of the TfL Group and such client; and

10.1.2 ensure that the personnel acting in any capacity for any such client are different from the personnel involved in performing this Agreement or in any other work which the Service Provider carries out in relation to any member of the TfL Group;

10.1.3 ensure that any personnel acting for any such client do not have access to information held by the Service Provider relating to any member of the TfL Group; and

10.1.4 inform the Authority of all such existing clients where there could be a conflict of interest and the steps that it is taking to ensure compliance with **clauses 10.1.1** to **10.1.3** inclusive.

10.2 The Service Provider shall undertake ongoing and regular conflict of interest checks throughout the duration of the Agreement and shall notify the Authority in writing immediately upon becoming aware of any actual or potential conflict of interest with the Services and shall work with the Authority or any member of the TfL Group to do whatever is necessary to manage such conflict to the TfL Group's satisfaction.

10.3 If the Service Provider is in breach of **clause 10.1** or if the Authority is not satisfied on the issue of any conflict of interest in accordance with **clause 10.2**, the Authority may terminate this Agreement and any other contracts

between the Service Provider and any member of the TfL Group immediately.

11. ACCESS TO THE AUTHORITY PREMISES

11.1 Any access to any Authority Premises made available to the Service Provider in connection with the proper performance of this Agreement shall be free of charge and shall be used by the Service Provider solely for the purpose of performing the Services during the term of this Agreement in accordance with this Agreement provided, for the avoidance of doubt, that the Service Provider shall be responsible for its own costs of travel including any congestion charging and/or low emission zone charging. The Service Provider, including the Service Provider's Personnel, shall:

11.1.1 have the use of such Authority Premises as licensee and shall not have or purport to claim any sole or exclusive right to possession or to possession of any particular part of such Authority Premises;

11.1.2 vacate such Authority Premises upon the termination of this Agreement or at such earlier date as the Authority may determine. If the Service Provider is asked to vacate the Authority Premises before the termination of this Agreement, the Service Provider shall not be liable for any delay in the supply of the Software or the performance of the Services to the extent so caused by the request to vacate (provided such request is not due to the Service Provider's breach or default);

11.1.3 not exercise or purport to exercise any rights in respect of any the Authority Premises in excess of those granted under this **clause 11**;

11.1.4 ensure that the Service Provider's Personnel carry any identity passes issued to them by the Authority at all relevant times; and

11.1.5 not damage the Authority Premises or any assets of the TfL Group.

11.2 Nothing in this **clause 11** shall create or be deemed to create the relationship of landlord and tenant in respect of any of the Authority Premises between the Service Provider and any TfL Group Member.

11.3 Unless agreed otherwise in writing between the parties (referencing this Agreement), the Authority shall be under no obligation to provide office or other accommodation or facilities or services (including telephony and IT services) to the Service Provider.

11.4 The Service Provider shall, while on the Authority Premises, comply with all of the TfL Group's security procedures and requirements notified to it from time to time, including the Security Policy, and shall ensure that all of the Service Provider's Personnel comply with all such procedures and requirements.

11.5 The Authority reserves the right, acting reasonably:

11.5.1 to refuse to admit to any of the Authority Premises any of the Service Provider's Personnel who fail to comply with any of the TfL Group's procedures, requirements, policies and standards referred to in **clause 12**;

11.5.2 to instruct any of the Service Provider's Personnel to leave any of the Authority Premises at any time and such Service Provider's Personnel shall comply with such instructions immediately.

11.6 The Service Provider shall promptly notify the Service Provider's Personnel and the Authority of any health and safety hazards that exist or may arise in connection with the performance of the Services.

12. **COMPLIANCE WITH POLICIES AND LAW**

12.1 The Service Provider undertakes to procure that all of the Service Provider's Personnel comply with all of the TfL Group's policies and standards that are relevant to the performance of the Services (including where the GLA is the Authority the GLA's Dignity at Work policy as updated from time to time and with the GLA's Code of Ethics as updated from time to time, and where TfL is

the Authority, TfL's workplace harassment policy as updated from time to time (copies of which are available on request from TfL) and with TfL's Code of Conduct (which is available on TfL's website, www.tfl.gov.uk)), including those relating to safety, security, business ethics, drugs and alcohol, the Security Policy, and any other on-site regulations specified by the Authority for personnel working at the Authority Premises or being granted access to the Sites in accordance with **clause 11**.   The Authority shall provide the Service Provider with copies of such policies and standards on request. In the event that the Services are being provided to both the GLA and TfL, then the policies and standards of each of the GLA and TfL shall apply as appropriate.

12.2   The TfL Group's workplace harassment policy as set out in **clause 12.1** (**"Policy"**) requires the TfL Group's own staff and those of its contractors to comply fully with the Policy to eradicate harassment in the workplace. The Service Provider shall:

12.2.1   ensure that its staff, and those of its sub-contractors, working on the Authority Premises are fully conversant with the requirements of the Policy;

12.2.2   fully investigate allegations of workplace harassment in accordance with the Policy; and

12.2.3   ensure that appropriate, effective action is taken where harassment is found to have occurred.

12.3   The Authority is committed to the improvement of business performance and the minimisation of risks and disruption to the TfL Group's and the Service Provider's respective employees, agents and subcontractors and customers of the TfL Group and those interfacing with the TfL Group transport networks through the effective management of health, safety and environmental issues and the Service Provider shall demonstrate its support for such commitment by:

12.3.1   implementing an effective health, safety and environmental management system; and

12.3.2   maximising opportunities for environmentally responsible procurement and maximising environmental opportunities and minimising environmental risks,

and shall communicate its methodology for doing so to the Authority.

12.4   If required by the Authority under **Schedule 1**, the parties shall agree an equality policy and if so, for the duration of this Agreement, the Service Provider shall comply with the Agreed Equality Policy.

12.5   Without prejudice to the generality of the foregoing, the Service Provider acknowledges that the Authority is under a duty:

12.5.1   where the Authority is TfL by virtue of a Mayor's direction under section 155 of the Greater London Authority Act 1999 (in respect of section 404(2) of the Greater London Authority Act 1999), and where the Authority is the GLA under section 404(2) of the Greater London Authority Act 1999, to have due regard to the need:

to promote equality of opportunity for all persons irrespective of their race, sex, disability, age, sexual orientation or religion;

to eliminate unlawful discrimination; and

to promote good relations between persons of different racial groups, religious beliefs and sexual orientation; and

12.5.2   under section 76A of the Sex Discrimination Act 1975 and section 71 of the Race Relations Act 1976, to have due regard to the need to eliminate unlawful discrimination on grounds of sex or marital status and/or race and to promote equality of opportunity and good relations between persons of different racial groups;

and, in providing the Services, the Service Provider shall assist and cooperate with the Authority and any TfL Group Member where possible to enable the Authority and any other TfL Group Member to satisfy its duty.

12.6   The Service Provider:

12.6.1 shall not unlawfully discriminate;

12.6.2 shall procure that the Service Provider's Personnel do not unlawfully discriminate; and

12.6.3 shall use reasonable endeavours to procure that its direct and indirect subcontractors do not unlawfully discriminate

in relation to the Services, within the meaning and scope of the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, the Employment Equality (Sexual Orientation) Regulations 2003, the Employment Equality (Religion or Belief) Regulations 2003, the Employment Equality (Age) Regulations 2006, and any other relevant enactments in force from time to time relating to discrimination in employment.

12.7   Without prejudice to **clauses 12.5** and **12.6**, the Service Provider shall:

12.7.1 assist and co-operate with the Authority where possible to enable the Authority to comply with its duties under section 1 and section 149 of the Equality Act 2010 as and when section 1 and/or section 149 come into force, including any amendment or re-enactment of section 1 or section 149, and any guidance, enactment, order, regulation or instrument made pursuant to these sections; and

12.7.2 where the GLA is the Authority:

12.1.7.1 comply with policies developed by the Authority with regard to compliance with the Authority's duties referred to

in **clauses 12.5**and **12.8.1** as are relevant to the Agreement and the Service Provider's activities;

12.7.2.2   obey directions from the Authority with regard to the conduct of the Services in accordance with the duties referred to in **clauses 12.5**and **12.8.1**;

12.7.2.3   assist, and consult and liaise with, the Authority with regard to any assessment of the impact on and relevance to this Agreement of the duties referred to in **clauses 12.5**and **12.8.1**;

12.7.2.4   on entering into any contract with a sub-contractor in relation to this Agreement, impose obligations upon the sub-contractor to comply with this **clause 12.7** as if the sub-contractor were in the position of the Service Provider;

12.7.2.5   provide to the Authority, upon request, such evidence as the Authority may require for the purposes of determining whether the Service Provider has complied with this **clause 12.7**. In particular, the Service Provider shall provide any evidence requested within such timescale as the Authority may require, and co-operate fully with the Authority during the course of the Authority's investigation of the Service Provider's compliance with its duties under this **clause 12.7**; and

12.7.2.6   inform the Authority forthwith in writing should it become aware of any proceedings brought against it in connection with this Agreement by any person for breach of the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, the Employment Equality (Sexual Orientation) Regulations 2003**,** the Employment Equality (Religion or Belief) Regulations 2003, or the Equality Act 2010.

12.8   If, pursuant to or in consequence of performing its obligations under this Agreement, the Service Provider gains access to any computer system of any TfL Group Member including any software, hardware, firmware, database, data or file, whether directly or remotely:

12.8.1   all access shall be strictly limited to that part of the computer software, hardware, firmware, database, data or files (as the case may be) as is required for proper performance of its obligations under this Agreement;

12.8.2   the Service Provider shall comply with all reasonable security audit and other procedures and requirements of any TfL Group Member in relation to access; and

12.8.3   the Service Provider shall ensure that only the Service Provider's Personnel shall be permitted access and such access shall be to the extent strictly necessary for the proper performance of their duties in relation to the obligations of the Service Provider pursuant to this Agreement.

12.9   In providing the Services, the Service Provider shall (taking into account best available techniques not entailing excessive cost and the best practicable means of preventing or counteracting the effects of any noise or vibration) have appropriate regard (insofar as the Service Provider's activities may impact on the environment) to the need to:

12.9.1   preserve and protect the environment and to the need to avoid, remedy and mitigate any adverse effects on the environment;

12.9.2   enhance the environment and have regard to the desirability of achieving sustainable development;

12.9.3   conserve and safeguard flora, fauna and geological or physiological features of special interest; and

12.9.4   sustain the potential of natural and physical resources and the need to safeguard the life-supporting capacity of air, water, soil and ecosystems.

12.10   Without limiting the generality of **clause 9.1.8**, the Service Provider shall comply with the Bribery Act 2010 and any guidance issued from time to time by the Secretary of State under it.

13.   CORRUPT GIFTS AND PAYMENT OF COMMISSION

13.1   The Service Provider shall not, and shall ensure that its employees, agents and sub-contractors do not, pay any commission or fees or grant any rebates to any employee, officer or agent of any TfL Group Member nor favour any employee, officer or agent of any TfL Group Member with gifts or entertainment of significant cost or value nor enter into any business arrangement with employees, officers or agents of any TfL Group Member other than as a representative of the Authority, without the TfL Group's prior written approval.

14.   EQUIPMENT

14.1   Risk in:

14.1.1   all of the Service Provider's Equipment shall be with the Service Provider at all times; and

14.1.2   all other equipment and materials forming part of the Services (**"Materials"**) shall be with the Service Provider at all times unless or until ownership and risk transfers in accordance with the **Annexes** to **Schedule 2** of this Agreement,

regardless of whether or not the Service Provider's Equipment and Materials are located at the Authority Premises.

14.2   The Service Provider shall ensure that all of the Service Provider's Equipment and all Materials meet all minimum safety standards required from time to time by law.

14.3   All of the Service Provider's Equipment which the Service Provider brings to the Authority Premises shall be removed by the Service Provider on termination of this Agreement and the Authority shall provide the Service Provider with such access to the Authority Premises as is reasonably required to enable such removal.

15.   **QUALITY AND BEST VALUE**

15.1   The Service Provider acknowledges that the Authority is a best value authority for the purposes of the Local Government Act 1999 and, as such, the Authority is required to make arrangements to secure continuous improvement in the way it exercises its functions, having regard to a combination of economy, efficiency and effectiveness.   Accordingly, the Service Provider shall, where reasonably requested by the Authority, participate in any relevant best value review and shall maintain an effective and economical programme for quality management, planned and developed in conjunction with any other functions of the Service Provider necessary to satisfy the requirement contemplated in this Agreement.

15.2   Where the GLA is the Authority then in accordance with the statutory requirement set out in section 61(3) of the Greater London Authority Act 1999, the Service Provider shall send such representatives as may be requested to attend the Greater London Assembly for questioning in relation to the Agreement.   The Service Provider acknowledges that it may be liable to a fine or imprisonment if it fails to comply with a summons to attend.

16.   **RECORDS, AUDIT AND INSPECTION**

16.1   The Service Provider shall, and shall procure that its sub-contractors shall:

16.1.1   maintain a complete and correct set of records pertaining to all activities relating to the performance of the Services and the Service Provider's obligations under this Agreement and all transactions entered into by the Service Provider for the purposes of this Agreement (including time-sheets for the Service Provider's Personnel where such records are material to the calculation of any sums due under this Agreement) (**"Records"**);and

16.1.2 retain all Records during the term of this Agreement and for a period of not less than six (6) years (or such longer period as may be required by law) following termination of this Agreement (**"Retention Period"**).

16.2 The Authority and any person nominated by the Authority has the right to audit any and all Records at any time during the Retention Period on giving to the Service Provider what the Authority considers to be reasonable notice (whether in writing or verbally) and at any reasonable time to inspect any aspect of the Service Provider's performance of the Services (including compliance with **clause 12**). The Authority shall use reasonable endeavours to co-ordinate its audits and to manage the number, scope, timing and method of undertaking audits so as to ensure that the Service Provider is not, without due cause, disrupted or delayed in the performance of its obligations under this Agreement.

16.3 The Service Provider grants to the Authority and its agents the right, at any time, on two (2) Business Days' notice, to audit and/or test the security and robustness of the Software, the Services and/or the Service Provider's compliance with the TfL Group's requirements on security, data integrity and protection against breach of confidentiality. Such audits and tests may include penetration testing and ethical hacking and the Service Provider grants consent for such tests and audits to be performed notwithstanding any provisions contained within the Computer Misuse Act 1990 or the Police and Justice Act 2006. In view of the fact that such audits and testing may be intended to simulate a criminal attack, the Service Provider agrees not to take any action against the TfL Group or its agents performing the audits or tests and that the TfL Group and their agents shall not be responsible or liable for any loss, damage, expenses or claims incurred by the Service Provider as a result of such tests or audits, including any loss or damage caused to the Service Provider's systems or the Service Provider's business or any third party claims brought against the Service Provider relating to or arising out of such tests or audits except to the extent that it would be unlawful for the Authority not to be responsible or liable. The Service Provider agrees to indemnify the TfL Group and its agents against any loss, damage

or expenses that the TfL Group or its agents may incur by reason of claims, actions, demands or proceedings brought against the TfL Group or its agents by third parties, including the Service Provider's suppliers, arising out of or in connection with such audits or tests.

16.4   For the purposes of exercising its rights under **clauses 16.2** and **16.3**, the Service Provider shall provide the Authority and/or any person nominated by the Authority with all reasonable co-operation including:

16.4.1   granting access to any premises, equipment, plant, machinery or systems used in the Service Provider's performance of this Agreement, and where such premises, equipment, plant, machinery or systems are not the Service Provider's own, using all reasonable endeavours to procure such access;

16.4.2   ensuring that appropriate security systems are in place to prevent unauthorised access to, extraction of and/or alteration to any Records;

16.4.3   making all Records available for inspection and providing copies of any Records if requested; and

16.4.4   making the Service Provider's Personnel available for discussion with the Authority.

16.5   Any audit, inspection and/or testing by the Authority pursuant to **clause 16.3** shall not relieve the Service Provider or any of its sub-contractors from any obligation under this Agreement or prejudice any of the TfL Group's rights, powers or remedies against the Service Provider.

16.6   The Service Provider shall promptly, to the extent reasonably possible in each particular circumstance, comply with the TfL Group's reasonable requests for access to senior personnel engaged in the Service Provider's performance of the Services.

16.7   This **clause 16** shall survive termination of this Agreement.

17. **CONTRACT MANAGEMENT AND CHANGE CONTROL**

17.1 The Service Provider shall provide the Authority with a written report on a monthly basis in respect of the Services performed in the preceding month or at the intervals set out in **Schedule 1**, if different. Such reports shall be provided within ten (10) Business Days of the end of the relevant calendar month or interval set out in **Schedule 1**. Unless agreed otherwise in writing, a review meeting shall be held within ten (10) Business Days thereafter between representatives of the parties to discuss such report and any other matters relating to the status and performance of this Agreement generally.

17.2 Any reports to be provided to the Authority under **clause 17.1** will contain at least the following and any other agreed items:

17.2.1 written status summary;

17.2.2 requests for action from the Authority;

17.2.3 activities completed during the period;

17.2.4 activities to be completed in the next period and by whom;

17.2.5 perceived risk factors and the strategies being used to minimise them; and

17.2.6 where applicable to the relevant Service(s) being provided, measurement of the Service Provider's performance against the Service Levels and details of any Service Credits accrued,

in a form to be agreed between the Authority and the Service Provider.

17.3 Any and all changes to the Services and the Software to be supplied shall be made in accordance with the Change Control Provisions set out in **Schedule 7**.

18. **INSURANCE**

18.1 The Service Provider shall at its sole cost obtain and maintain the Insurances.

18.2 The Service Provider shall:

18.2.1 procure that its public liability insurance extends to indemnify the Authority as principal;

18.2.2 procure the Authority's interest is noted on each and every policy or that its public liability insurance, employer's liability insurance and product liability insurance includes an Indemnity to Principal clause;

18.2.3 where requested by the Authority, provide evidence satisfactory to the Authority prior to the Commencement Date and at least five (5) Business Days prior to each anniversary of the Commencement Date that the Insurances have been effected and are in force. Where requested by the Authority, the Service Provider shall within five (5) Business Days after the date of renewal of any Insurance provide the Authority with satisfactory evidence that such Insurance has been renewed;

18.2.4 where the Insurances contain a care, custody or control exclusion, procure that the relevant policy is endorsed so as to delete the exclusion in respect of any of the Authority Premises (including contents) that are occupied by the Service Provider for the purpose of performing the Services;

18.2.5 if required by the Authority, procure that prior to cancelling or changing any term of any Insurances, such that it no longer meets the requirements set out in this Agreement, the insurer or insurers under such Insurances give the Authority not less than thirty (30) days' notice of intention to cancel or make such change;

18.2.6 bear the cost of all or any excesses under the Insurances;

18.2.7 notify the Authority as soon as reasonably practicable in writing of any anticipated or actual event or circumstance which may lead or

has led to any Insurance lapsing or being terminated or the cover under it being reduced or modified;

18.2.8 notify the Authority as soon as reasonably practicable in writing upon becoming aware of any claim, event or circumstance which is likely to give rise to any claim or claims in aggregate in respect of the Services in excess of £100,000 or the figure set out in **Schedule 1**, if different, on any Insurance and, if requested by the Authority and where not otherwise subject to an obligation of confidentiality, provide full details of such claim, event or circumstance (and such other relevant information as the Authority may reasonably require) within three (3) Business Days of the TfL Group's request;

18.2.9 promptly and diligently deal with all claims under the Insurances (or any of them) relating to the Services and in accordance with all insurer requirements and recommendations; and

18.2.10 in relation to any claim settled under the Insurances in respect of the Services and to the extent that the proceeds of such claim are payable to the Service Provider, pay the proceeds to the person who suffered the loss or damage that gave rise to the claim (whether the Authority, a TfL Group Member or any third party).

18.3 If the Service Provider is in breach of **clause 18.2** and does not remedy such breach within thirty (30) days of notice from the Authority to do so, then without prejudice to any of its other rights, powers or remedies, the Authority may pay any premiums required to keep any of the Insurances in force or itself procure such Insurances. In either case, the Authority may recover such premiums from the Service Provider, together with all expenses incurred in procuring such Insurances as a debt.

18.4 The Service Provider warrants that nothing has or will be done or be omitted to be done which may result in any of the Insurances being or becoming void, voidable or unenforceable.

18.5   In relation to Insurances which must be held for a period which extends beyond termination, this **clause 17.3** shall survive termination of this Agreement.

19.   **THE TFL GROUP'S DATA**

19.1   The Service Provider acknowledges the TfL Group's ownership of Intellectual Property Rights which may subsist in the TfL Group's data. The Service Provider shall not delete or remove any copyright notices contained within or relating to TfL Group's data.

19.2   The Service provider shall at any time when any of the TfL Group's data is in its control or possession preserve the integrity of such TfL Group's data and to prevent any corruption or loss of TfL Group's data.

20.   **INTELLECTUAL PROPERTY RIGHTS**

20.1   Except for any of the Service Provider's Software, the Third Party Software, the Service Provider's IPR and Third Party IPR, all Intellectual Property Rights of whatever nature in the Software and the Services (**"the Authority Rights"**) whether created by the Service Provider or any of the Service Provider's Personnel shall or shall on creation of the same be and remain vested in the Authority. Prior to such vesting, the Service Provider grants the TfL Group a non-exclusive, perpetual, royalty-free, worldwide and licence to use, adapt, translate, support and sub-licence the Authority Rights to the extent necessary for the Authority, the TfL Group and its other authorised agents to receive its rights under this Agreement, including with respect to the right to test the Software and/or Services. The Service Provider shall do all such acts and execute all such deeds and documents as shall be necessary or desirable to perfect the right, title and interest of the Authority in and to such Intellectual Property Rights, including ensuring that the Service Provider's Personnel assign all such Intellectual Property Rights owned by them either direct to the Authority or to the Service Provider to enable the Service Provider to comply with its obligations hereunder and waive any moral rights they may otherwise have, in each case at no cost to the Authority.

20.2	Nothing in this **clause 20** shall prevent the Service Provider from using data processing techniques, ideas and know-how gained during the performance of this Agreement in the furtherance of its normal business, to the extent that this does not constitute or relate to a disclosure of Confidential Information or an infringement by the Service Provider of any Intellectual Property Right.

20.3	To the extent that any TfL Group Member provides the Service Provider for the purpose of or in connection with providing the Services or supplying the Software with any materials in which any TfL Group Member owns (or is licensed by a third party to use) the Intellectual Property Rights, the Service Provider acknowledges and agrees that nothing in this Agreement grants to the Service Provider any right, title or interest in such materials other than a limited non-exclusive right to use those materials solely for the purposes of providing the Services. All Intellectual Property Rights in such materials are and shall remain the exclusive property of the TfL Group Member or (if applicable) its third party licensors.

20.4	The Service Provider warrants and shall ensure that the possession and/or use by the TfL Group of the Software, and the performance by the Service Provider of the Services shall not constitute any infringement or misappropriation of any Intellectual Property Rights or any other legal or equitable right of any person and that the Service Provider owns or has obtained valid licences to or of all such Intellectual Property Rights and other rights which are necessary for the performance of its obligations under this Agreement.

20.5	If any third party claims that the possession and/or use of the Software and/or the receipt of the Services (**"Indemnified Deliverables"**) by any TfL Group Member and/or the provision by the Service Provider of any Indemnified Deliverable under or in connection with this Agreement constitutes an infringement or misappropriation of any Intellectual Property Rights or other right of that third party (**"IPR Claim"**), the Service Provider shall indemnify, keep indemnified and hold harmless the TfL Group Members (including their respective employees, sub-contractors and agents) from and

against all Losses arising from or incurred by reason of any such IPR Claim (including the defence and any settlement of such IPR Claim).

20.6 In the event of a claim pursuant to **clause 20.5**:

20.6.1 the Authority shall promptly notify the Service Provider of the claim;

20.6.2 the Service Provider shall, at its own cost and expense, control the defence of such IPR Claim and any related proceedings or settlement negotiations, except that the Authority shall be entitled to take any action which it deems necessary if the Service Provider fails to take action, or (in the TfL Group's reasonable opinion) delays taking action, in defending or settling any such IPR Claim and such failure or delay may, in the reasonable opinion of the Authority, prejudice the interests of the TfL Group; and

20.6.3 at the cost and expense of the Service Provider, the Authority shall take all reasonable steps to co-operate with the Service Provider in the defence or settlement of such IPR Claim.

20.7 If any Indemnified Deliverable becomes the subject of any IPR Claim and, as a result of such IPR Claim, a court of competent jurisdiction grants an injunction preventing the use by the Service Provider or any TfL Group Member of any of such Indemnified Deliverable or there is substantial risk of such injunction being granted or the IPR Claim is settled on the basis that the Indemnified Deliverable cannot be used, the Service Provider shall at its expense as soon as possible following (and in any event within thirty (30) days of) such event occurring:

20.7.1 obtain for the TfL Group Members the right to continue to possess, use and/or receive the benefit of the relevant Indemnified Deliverable(s); or

20.7.2 replace or modify the relevant Indemnified Deliverable(s) so that it becomes non-infringing without detracting from the functionality or performance of the overall Software or Service and provided that any

such replacement or modification shall not prevent the Service Provider's compliance with the warranties contained at **clause 9**.

20.8   The Service Provider shall have no liability under or in connection with this Agreement for any infringement caused solely and directly by:

20.8.1   the combination of the relevant Indemnified Deliverable with other products, data or information not supplied by the Service Provider unless the combination was made or approved by the Service Provider;

20.8.2   the modification of the Indemnified Deliverable unless the modification was made or approved by the Service Provider;

20.8.3   the supply by or on behalf of the Authority of any of the materials specified at **clause 20.3**; or

20.8.4   breach by the Authority of any of the terms of this Agreement and/or any licence terms in respect of the Indemnified Deliverable to which the Authority is subject pursuant to the terms of this Agreement.

20.9   If any third party claims that the possession and/or use by the Service Provider of any of the materials provided to the Service Provider as contemplated in **clause 20.3** (the **"Authority Deliverables"**) constitutes an infringement or misappropriation of any Intellectual Property Rights or other right of that third party, the Authority shall indemnify, keep indemnified and hold harmless the Service Provider (including their respective employees, sub-contractors and agents) from and against all claims, demands, actions, costs, expenses (including legal costs and disbursements on a full indemnity basis) and damages awarded by a court of competent jurisdiction or agreed to be paid by way of settlement of such claim provided that:

20.9.1   the Service Provider promptly notifies the Authority of such claim;

20.9.2   the Authority shall, at its own cost and expense, be entitled to control the defence of such claim and any related proceedings or settlement negotiations; and

20.9.3 at the cost and expense of the Authority, the Service Provider takes all reasonable steps to co-operate with the Authority in the defence or settlement of such claim.

20.10 The Authority shall not be liable under **clause 20.9** or otherwise for any infringement:

20.10.1 caused by the combination of the relevant Authority Deliverables with other products, data, or information not supplied by the Authority;

20.10.2 caused by any use by the Service Provider of any of the Authority Deliverables other than strictly for the purpose of the Service Provider performing its obligations under this Agreement; or

20.10.3 caused by breach by the Service Provider of any of the terms of this Agreement.

20.11 If any of the Authority Deliverables become the subject of any claim as described in **clause 20.9** and, as a result of such claim, a court of competent jurisdiction grants an injunction preventing the TfL Group's and/or the Service Provider's use of any such of the Authority Deliverables or there is substantial risk of such injunction being granted or the claim is settled on the basis that the Authority Deliverables cannot be used, the Authority shall at its expense as soon as possible following (and in any event within thirty (30) days of) such event occurring:

20.11.1 obtain for the Service Provider the right to continue to possess and/or use the relevant Authority Deliverables;

20.11.2 with all such assistance from the Service Provider (including the provision of Additional Services) as may be agreed in accordance with **clause 32**, replace or modify the relevant Authority Deliverables so that it becomes non-infringing without detracting from the functionality or performance of the Authority Deliverables so as to prevent the Service Provider from complying with its obligations under this Agreement; or

20.11.3 if it is not commercially reasonable to perform either of the above options, the Authority and the Service Provider shall cease use of the infringing the Authority Deliverables in which case the parties' representatives shall meet and, in good faith, explore all possible amendments to the Services which are required as a result of such cessation of use. Any such amendments shall be considered and (where applicable) agreed in accordance with **clause 32**.

20.12 The Service Provider shall ensure that all royalties, licence fees or similar expenses in respect of all Third Party IPR used in connection with this Agreement have been paid and no such amounts shall be payable by the Authority or any TfL Group Member except to the extent such amounts are included within the Charges.

20.13 This **clause 20** shall survive termination of this Agreement.

21. **GENERAL EXCLUSIONS AND LIMITATIONS OF LIABILITY**

21.1 Neither party excludes or limits its liability to the other party in respect of:

21.1.1 the terms implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982;

21.1.2 death or personal injury resulting from negligence within the meaning of section 1(1) of the Unfair Contract Terms Act 1977;

21.1.3 to the extent applicable, liability under Part 1 of the Consumer Protection Act 1987 for defects within the meaning of that Act;

21.1.4 **clause 29** (Confidentiality and Transparency);

21.1.5 fraud (including fraudulent misrepresentation); or

21.1.6 any other liability which, by law, it cannot exclude or limit,

but nothing in this clause confers any right or remedy upon a party to which it would not otherwise be entitled.

21.2 The Service Provider does not exclude or limit its liability to the Authority under or in connection with this Agreement:

21.2.1 for breach of Intellectual Property Rights (whether pursuant to **clause 20** (Intellectual Property Rights) or otherwise);

21.2.2 in respect of liability pursuant to **clause 11** (Access to the Authority Premises);

21.2.3 in respect of liability pursuant to **clauses 30 and 31**30.4 (Freedom of Information and Data Protection); or

21.3 Subject to **clauses 21.1** and **21.2**, **clauses 21.3** to **21.8** set out the entire liability of each party (including liability for the acts or omissions of its employees, agents or sub-contractors and, in relation to the Authority, the acts or omissions of the TfL Group) to the other party in respect of:

21.3.1 any breach of its contractual obligations arising under or in connection with this Agreement;

21.3.2 any representation, statement, negligence, breach of statutory duty or other tortious act or omission arising under or in connection with this Agreement; and

21.3.3 any damage to property.

21.4 Except as provided in **clauses 21.1** and **21.2**, the Service Provider's maximum liability under this Agreement will be as set out in **Schedule 1**.

21.5 Except as provided in **clause 21.1**, the entire liability of the Authority and the TfL Group (together) under or in connection with this Agreement will not exceed the TfL Group's Liability Cap.

21.6 In the event that a TfL Group Member other than the Authority suffers Losses in circumstances where the Authority would be able to recover such Losses from the Service Provider, such person may recover from the Service Provider an amount equal to the amount that the Authority would have been able to recover had the Losses been suffered by the Authority rather than the

other TfL Group Member subject always to the limitations and exclusions of liability contained in this Agreement. In the alternative, the Service Provider agrees that any Losses suffered or incurred by any TfL Group Member arising under or in connection with this Agreement (in this **clause 21.6** collectively **"Group Member Losses"**): (i) will be deemed to have been incurred by the Authority; and (ii) will be recoverable by the Authority from the Service Provider as if they were losses suffered or incurred directly by the Authority but always subject to the limitations and exclusions of liability set out in this Agreement.   For the purposes of this **clause 21.6**, any TfL Group Member Losses shall not be deemed to be consequential or indirect or special merely as a result of not being suffered directly by the Authority. For the avoidance of doubt, the Service Provider shall still be entitled, in the case of a remediable breach, to remedy such breach in accordance with the terms of this Agreement.

21.7   In the event that the Service Provider is defined under this Agreement to include more than one person, then each such person shall be jointly and severally liable for all obligations of the Service Provider under this Agreement.

21.8   The exclusions from and limitations of liability set out in this **clause 21** shall be considered severably. The validity or unenforceability of any one clause, sub-clause, paragraph or sub-paragraph of this **clause 21** shall not affect the validity or enforceability of any other clause, sub-clause, paragraph or sub-paragraph of this **clause 21**.

21.9   Subject to **clause 21.10**, the Service Provider is responsible for and shall indemnify, keep indemnified and hold harmless the Authority and the other TfL Group Members (including their respective employees, sub-contractors and agents) (the **"Indemnified Party"**) against all Losses which the Indemnified Party incurs or suffers as a consequence of any breach or any negligent performance of this Agreement by the Service Provider (including in each case any non-performance or delay in performance of this Agreement) or of any breach of statutory duty, misrepresentation or misstatement by the Service Provider.

21.10 The Service Provider is not responsible for and shall not indemnify the Authority for any Losses to the extent that such Losses are caused by any breach or negligent performance of any of its obligations under this Agreement by the Authority and/or any other the TfL Group Member.

21.11 The provisions of this **clause 21** shall survive the termination of the whole or a part of this Agreement.

22. **FORCE MAJEURE**

22.1 Neither party shall be liable for any delay in performing or for failure to perform any of its obligations under this Agreement due to a Force Majeure Event.

22.2 If either party is prevented from performing any of its obligations due to a Force Majeure Event it shall promptly notify the other party in writing of the circumstances of the Force Majeure Event and the other party shall grant a reasonable extension for the performance of this Agreement. The other party shall in no circumstances be obligated to give an extension which is of a period longer than the Force Majeure Period set out in **Schedule 1**. The Authority may terminate this Agreement on immediate notice in writing if a Force Majeure Event affecting the Service Provider continues for more than the Force Majeure Period set out in **Schedule 1**.

22.3 It is expressly agreed that any failure by the Service Provider to perform, or any delay by the Service Provider in performing, its liabilities, obligations or responsibilities under this Agreement which results from any failure or delay in the performance of its obligations by any person with which the Service Provider shall have entered into any contract, supply arrangement, sub-contract or otherwise, shall be regarded as a failure or delay due to a Force Majeure Event only in the event that such person shall itself be prevented from or delayed in complying with its obligations under such contract, supply arrangement, sub-contract or otherwise as a result of circumstances of a Force Majeure Event.

22.4 Not used

23. **LOSS OF SOFTWARE AND DATA SECURITY**

23.1 Without prejudice to its other obligations under this Agreement, the Service Provider shall, during the term of this Agreement and in the course of performing the Services, provide all measures necessary in respect of the prevention of unauthorised access to any TfL Group Member's computer systems, software and data, the prevention of the introduction of known Viruses and shall provide the capability to restore the systems, software and data in the event that the loss of the systems, software or data arises directly or indirectly from any act or omission of the Service Provider (including the Service Provider's Personnel) or whilst such systems, software or data is in the custody, control or otherwise interfaced with or accessed by the Service Provider.

23.2 The Service Provider shall not, without the consent of the Authority, be entitled to delete any software or data belonging to any TfL Group Member to which the Service Provider has access in performance of its obligations under this Agreement.

23.3 Upon receipt or creation by the Service Provider of the TfL Group's data and during any collection, processing, storage and transmission by the Service Provider of the TfL Group's software or data the Service Provider shall take all necessary precautions to preserve the integrity of such software and data and to prevent any corruption or loss thereof including such precautions as are specified by the Authority from time to time.

23.4 In the event that any of the TfL Group's software or data is corrupted or lost or so degraded as to be unusable due to any act or omission of the Service Provider after its receipt or creation by the Service Provider or during any collection, processing, storage or transmission by the Service Provider of the TfL Group's software or data or otherwise as a result of any default by the Service Provider then, in addition to any other remedies that may be available to the Authority under this Agreement or otherwise:

23.4.1 the Service Provider shall promptly, at the Service Provider's expense, restore or procure the restoration of the TfL Group's

software and data to the TfL Group's reasonable satisfaction, as notified in writing, such that the Service Provider has made good the corruption, loss or degradation of the software and data; and

23.4.2 in the event that the Authority itself has to restore or procure the restoration of the Service Provider's software or data, then the Authority shall require the Service Provider to repay the Authority's reasonable costs and expenses incurred in carrying out such restoration.

23.5 In the event that any of the TfL Group's software or data is corrupted or lost or sufficiently degraded as to be unusable otherwise than due to a default by the Service Provider, the Service Provider shall nevertheless carry out such remedial actions to restore the TfL Group's software and data or such other actions as may be necessary to restore the TfL Group's software and data as the Authority may request in writing and the reasonable agreed cost of the remedial actions or such other actions shall be borne by the Authority.

23.6 Without prejudice to the generality of **clauses 23.1** and **23.3**, the Service Provider shall:

23.6.1 before performing any actions in respect of any TfL Group Member's software or data, ensure that it has performed back-ups of such software or data as set out in **Schedule 1** or agreed in writing from time to time or, where none are agreed, as are reasonable in the circumstances; and

23.6.2 perform its obligations in conformance with the Security Policy.

Nothing in this Agreement shall relieve the Service Provider's obligations in this regard.

23.7 The Service Provider shall fully indemnify the Authority and the TfL Group for any and all Losses incurred or suffered by the Authority and/or any the TfL Group Member which results from a breach by the Service Provider of its obligations under this **clause 23**.

23.8   This **clause 23** shall survive termination of this Agreement.

24.   **TERMINATION**

24.1   Without prejudice to the TfL Group's right to terminate at common law, the Authority may terminate this Agreement immediately (or on such later date as it shall specify in writing) upon giving notice to the Service Provider if:

24.1.1   the Service Provider has committed any material or persistent breach of this Agreement and in the case of such a breach that is capable of remedy fails to remedy that breach within twenty (20) Business Days from the date of written notice to the Service Provider giving details of the breach and requiring it to be remedied;

24.1.2   the Service Provider is subject to an Insolvency Event;

24.1.3   there is a Change of Control or of management personnel of the type referred to in **clause 28.4**; or

24.1.4   the Authority is not satisfied on the issue of any conflict of interest in accordance with **clause 10**;

24.1.5   the Service Provider commits any of the money laundering offences under the Money Laundering Regulations 2003;

24.1.6   the Service Provider or any of its officers, employees, sub-contractors or agents commits any act of bribery described in the Bribery Act 2010; or

24.1.7   a termination circumstance, as referred to in **Schedule 6**, applies.

24.2   Without prejudice to the TfL Group's right to terminate this Agreement under **clause 24.1** or to terminate at common law, the Authority may, subject to **clause 25.10** and **clause** 25.11, terminate this Agreement and/or the Maintenance Services and/or the Additional Services at any time following Go-Live without cause subject to giving the Service Provider written notice of the period specified in **Schedule 1**.

24.3 To the extent that the Authority has a right to terminate this Agreement under this **clause 24** then, as an alternative to termination, the Authority may by giving notice to the Service Provider require the Service Provider to provide part only of the Software or the Services set out in the **Annexes** to **Schedule 2** with effect from the date specified in the TfL Group's notice ("**Change Date**") whereupon the provision of the remainder of the Software or the Services will cease and the definition of "**the Software**" and/or "**the Services**" shall be deemed amended accordingly. The Charges applicable with effect from the Change Date will be adjusted proportionately or, if in the TfL Group's opinion a proportionate adjustment would not be reasonable, in such manner as the Authority may reasonably determine.

24.4 Subject to **clause 4.9**, the Service Provider may terminate for non-payment by the Authority. Termination may only occur after a failure to remedy by the Authority within sixty (60) Business Days from the date of written notice by the Service Provider provided that the Service Provider also provides a written notice to the Authority thirty (30) Business Days after the first written notice is served of its intention to terminate if payment is not made within the next thirty (30) Business Days.

24.5 Without prejudice to the Authority's right to terminate the Agreement under **clauses 24.1**, **24.2** or at common law, the Authority may terminate the Agreement at any time following a Declaration of Ineffectiveness in accordance with the provisions of **clause 25A**.

25. **CONSEQUENCES OF TERMINATION/EXIT**

25.1 Except in the case of termination for breach, the Service Provider shall provide the Authority with a statement of account of monies owing to it (if any) for agreement with the Authority. The statement will not include monies withheld under **clause 4.8** or **4.9**.

25.2 On termination of this Agreement, howsoever caused, clauses and Schedules in this Agreement which expressly or impliedly have effect after termination shall remain in effect including **clause 20** (Intellectual Property Rights), **clause 21** (General Exclusions and Limitations of Liability), **clause**

2928.5 (Confidentiality and Transparency), **clause 38** (Law and Dispute Resolution) and **Schedule 10** (Exit Management).

25.3 The termination of this Agreement shall not prejudice or affect any right, power or remedy which has accrued or shall accrue to either party prior to or after such termination.

25.4 Upon termination of this Agreement (howsoever caused) the parties shall perform their respective obligations under **Schedule 10** and the Exit Plan.

25.5 Notwithstanding the provisions of the Exit Plan and **Schedule 10**, whenever the Authority chooses to put out to tender for a replacement service provider for some or all of the Services or Software, the Service Provider shall disclose to tenderers such information concerning the Services and Software as the Authority may require for the purposes of such tender. The Service Provider may impose upon any recipient of such information such obligations of confidentiality as it may reasonably require.

25.6 The Authority shall, within thirty (30) days of the statement of accounts being agreed under **clause 25.1**, pay the Service Provider any charges remaining due in relation to any Services properly performed and/or the Software properly delivered in accordance with this Agreement up to the date of termination.

25.7 If the Authority terminates this Agreement other than under **clause 24.2**, then the Authority may, without prejudice to its other rights under this Agreement:

25.7.1 itself complete the supply of the Software and/or the Services, or enter into a contract with a third party to effect such completion and, for the avoidance of doubt, such completion shall be taken to include the creation or procurement of any software; and

25.7.2 the Authority shall be entitled to use or have used on its behalf all know-how and Intellectual Property Rights owned or controlled by the Service Provider used in or in connection with the Software and/or Services (including any Escrow Materials and Source Materials as defined below) free of charge for the purposes of completion and

use, amendment, modification and/or enhancement of the Software and Services as envisaged by this Agreement after such completion.

25.8   If the Authority terminates this Agreement in accordance with **clause 24.1.2**, then the Service Provider shall, as of the date of termination of this Agreement, assign to the TfL Group with full title guarantee, all Intellectual Property Rights in the Services and the Software which were due to be transferred to the Authority should the Insolvency Event have not occurred and which are in existence and capable of assignment as of the date of termination.

25.9   Upon termination of this Agreement (howsoever caused) or a cessation of any Services or part thereof, the Authority may enter into any agreement with any third party or parties as the Authority thinks fit to provide any or all of the Services and the Software and, save in the case of a termination by the Authority pursuant to **clause 24.2**, the Authority may recover from the Service Provider all additional expenditure reasonably incurred in making other arrangements for having services carried out, provided that the Authority shall take all reasonable steps to mitigate such incremental expenditure. The Authority may deduct such costs from the charges or any other sums due to the Service Provider or otherwise recover such costs from the Service Provider as a debt.

25.10   Where the Agreement is terminated under **clause 24.2** before the fifth (5) anniversary of Go Live, the Authority shall pay the Service Provider an Early Termination Charge of £65,000.

25.11   If the Authority terminates the Agreement under **clause 24.2** prior to Go-Live, the Authority shall pay the Service Provider an amount equal to:

a) fair and reasonable proportion of the amount equal to any expenditure reasonably incurred by the Service Provider in the expectation of completing the Services up to Go Live, in so far as such expenditure has not been recovered by the Service Provider, (whether through the Charges or otherwise) and which would reasonably have been expected to be recovered as part of the

Charges properly incurred under this Agreement up to Go Live. The Service Provider shall take all reasonable steps to minimise and to mitigate such expenditure.

25A   DECLARATION OF INEFFECTIVENESS

25A.1   In the event that a court makes a Declaration of Ineffectiveness, the Authority shall promptly notify the Service Provider. The parties agree that the provisions of **Clause 25** and this **Clause 25A** shall apply as from the date of receipt by the Service Provider of the notification of the Declaration of Ineffectiveness. Where there is any conflict or discrepancy between the provisions of **Clause 25** and this **Clause 25A** or the Cessation Plan, the provisions of this **Clause 25A** and the Cessation Plan shall prevail.

25A.2   The Declaration of Ineffectiveness shall not prejudice or affect any right, liability or remedy which has accrued or shall accrue to either Party prior to or after such Declaration of Ineffectiveness.

25A.3   As from the date of receipt by the Service Provider of the notification of the Declaration of Ineffectiveness, the parties (acting reasonably and in good faith) shall agree or, in the absence of such agreement, the Authority shall reasonably determine an appropriate Cessation Plan with the object of achieving:

25A.3.1   an orderly and efficient cessation of the Services or (at the Authority's request) a transition of the Services to the Authority or such other entity as the Authority may specify; and

25A.3.2   minimal disruption or inconvenience to the Authority or to public passenger transport services or facilities,

in accordance with the provisions of this **Clause 25A** and to give effect to the terms of the Declaration of Ineffectiveness.

25A.4   Upon agreement, or determination by the Authority, of the Cessation Plan the parties will comply with their respective obligations under the Cessation Plan.

25A.5 The Authority shall pay the Services Provider's reasonable costs in assisting the Authority in preparing, agreeing and complying with the Cessation Plan. Such costs shall be based on any comparable costs or Charges agreed as part of this Agreement or as otherwise reasonably determined by the Authority. Provided that the Authority shall not be liable to the Service Provider for any loss of profit, revenue, goodwill or loss of opportunity as a result of the early termination of this Agreement pursuant to this **Clause 25A**.

26. **STEP IN RIGHTS**

26.1 If the Authority reasonably believes that it needs to take action in connection with part or all of the Services:

26.1.1 because of a serious risk to the health or safety of persons or property or to the environment;

26.1.2 to discharge a statutory duty;

26.1.3 because the Services are not being performed to at least the Service Levels;

26.1.4 because the Services are not being performed when due to be performed; and/or

26.1.5 because the Services are not being performed in accordance with the terms of this Agreement,

then, save where such failure to perform is due to the acts or omissions of the Authority or any TfL Group Member and without prejudice to any other rights of the Authority, the provisions set out in this **clause 26** shall apply.

26.2 The Authority shall notify the Service Provider in writing of the following:

26.2.1 the action it wishes to take, which may include stepping-in to provide the affected services by the TfL Group or via a third party;

26.2.2 the reason for such action;

26.2.3 the date it wishes to commence such action;

26.2.4 the time period which it believes will be necessary for such action; and

26.2.5 to the extent practicable, the effect on the Service Provider and its obligations to provide the Services during the period such action is being taken.

26.3 Following service of such notice, the Authority or a third party appointed by the Authority for the purpose shall take such action as is notified under **clause 26.2** and any consequential additional action as the Authority reasonably believes is necessary (the **"Required Action"**) and the Service Provider shall give all reasonable assistance at no additional cost to the Authority or such third party while it is taking such the Required Action.

26.4 Without prejudice to the generality of **clause 26.3**, the Service Provider will co-operate fully with and provide all reasonable assistance to the Authority and/or third party performing the Required Action (**"Step-In Provider"**), including allowing:

26.4.1 the Step-In Provider to use all or any part of the Software and/or provide such access to the Service Provider's premises as may be reasonably required to assist in the performance of such Services;

26.4.2 the Step-In Provider reasonable access to such management records, software, documentation and equipment which relate to the Services as is reasonably necessary to enable the performance of the Services; and

26.4.3 the Step-In Provider to manage the Service Provider's business and contractual relationships with sub-contractors, agents and/or third party providers where relevant to the continuing provision of the Services.

26.5 The Step-In Provider will cease to provide the Services and the Service Provider will resume its obligations under this Agreement when the Service Provider can demonstrate to the reasonable satisfaction of the Authority that the Service Provider has rectified the breach that led to the appointment of

the Step-In Provider or the Authority confirms it wishes to cease providing the Required Action.

26.6 For so long as and to the extent that the Required Action is taken and this prevents the Service Provider from providing any part of the Services, the Service Provider shall be relieved from its obligations to provide such part of the Services and the Authority shall not be liable to pay Charges for such part of the Services.

26.7 The Service Provider will bear all of the reasonable costs and expenses of the Authority and any third party (including, amongst other things, staff costs) in taking the Required Action and any actions required to be taken by the Authority or such third party to re-transfer the obligation to provide the Services to the Service Provider.

26.8 Before the Authority exercises its right of step-in under this **clause 26** it shall permit the Service Provider the opportunity to demonstrate to the Authority's reasonable satisfaction within 5 Working Days that the Service Provider is still able to provide the Services in accordance with the terms of this Agreement and/or remedy the circumstances giving rise to the right to step-in without the requirement for the Authority to take action.

27. **SEVERABILITY**

27.1 If any provision of this Agreement (in whole or in part) is held to be invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed from this Agreement and the remaining provisions shall continue in full force and effect as if this Agreement had been executed without the invalid, illegal, or unenforceable provision. In the event that in the TfL Group's reasonable opinion such a provision is so fundamental as to prevent the accomplishment of the purpose of this Agreement, the Authority and the Service Provider shall immediately commence good faith negotiations to remedy such invalidity.

28. **ASSIGNMENT/SUB-CONTRACTING/CHANGE OF OWNERSHIP**

28.1 The Service Provider shall not assign or sub-contract all or any part of the Services or its obligations in relation to providing the Software without the

prior written consent of the Authority as to the identity of the relevant sub-contractor, which may be refused or granted consent subject to such conditions as the Authority sees fit.

28.2 Where the Service Provider sub-contracts all or any part of the Services or the provision of the Software to any person, the Service Provider shall:

28.2.1 ensure that such person is obliged to comply with all of the obligations and duties of the Service Provider under this Agreement insofar as they relate to the Services or the provision of the Software or part thereof (as the case may be) which that sub-contractor is required to provide;

28.2.2 be solely responsible for payments to that person;

28.2.3 remain solely responsible and liable to the Authority for any breach of this Agreement or act or omission of a sub-contractor or any performance, non-performance, part performance or delay in performance of any of the Services and/or obligations by any sub-contractor to the same extent as if such breach or act or omission had been made by the Service Provider;

28.2.4 without prejudice to the provisions of **clause 12**, ensure compliance with the Bribery Act 2010 and any guidance issued by the Secretary of State under it when appointing any such sub-contractor; and

28.2.5 where the GLA is the Authority, include a term in each sub-contract requiring payment to be made by the Service Provider to the sub-contractor within a specified period not exceeding 30 days from receipt of a valid invoice as defined by the sub-contract requirements.

28.3 Where the Authority gives its consent to sub-contracting under **clause** 28, the Authority may as a condition of giving its consent to the Service Provider require direct warranties, undertakings, guarantees and/or indemnities from such sub-contractor concerning the

provision of the Services and its compliance with the obligations set out in this Agreement in all respects.

28.4 The Service Provider shall give notice to the Authority within ten (10) Business Days in the event that there is:

28.4.1 any change in the control of the Service Provider where such change relates to fifty percent (50%) or more of the issued share capital of the Service Provider; or

28.4.2 any change in the control of the Holding Service Provider where such change relates to fifty percent (50%) or more of the issued share capital of the Holding Service Provider; or

28.4.3 in the case of an unincorporated Service Provider, any change in the management personnel of the Service Provider which alone or taken with any other change in management personnel not previously notified to the Authority, equates to a change in the identity of fifty percent (50%) or more of the management personnel of the Service Provider,

such notice to be given:

28.4.4 as soon as reasonably possible upon the Service Provider becoming aware the change of control or of management personnel is going to take place (taking into account any restrictions placed on giving such notice by any recognised stock exchange); and

28.4.5 within ten (10) Business Days of the date on which such change takes effect.

28.5 The Authority may novate or otherwise transfer this Agreement (in whole or in part). Within ten (10) Business Days of a written request from the Authority, the Service Provider shall, at its own expense, execute such agreement as the Authority may reasonably require to give effect to any such transfer of all or part of its rights and obligations under this Agreement to one or more persons nominated by the Authority.

29. **CONFIDENTIALITY AND TRANSPARENCY**

29.1 The Service Provider agrees in respect of Confidential Information disclosed pursuant to this Agreement or discovered further to the operation of this Agreement:

29.1.1 to keep the Confidential Information in strict confidence and secrecy;

29.1.2 not to use the Confidential Information save for complying with its obligations under this Agreement;

29.1.3 subject to **clause 29.1.4**, not to disclose the Confidential Information to a Third Party without prior written consent of the Authority (save that the Service Provider may disclose Confidential Information to any sub-contractors it appoints pursuant to **clause** 28. who of necessity need the same in the performance of this Agreement subject to such sub-contractor providing the Authority with an undertaking to keep the Confidential Information disclosed to it confidential in similar terms to the provisions of this **clause 29**); and

29.1.4 to restrict the disclosure of the relevant and necessary parts of the Confidential Information to such of its employees, agents and sub-contractors (including persons who are appointed from time to time by the Authority to maintain the Software) who of necessity need the same in the performance of this Agreement and in such circumstances to ensure that such employees, agents and sub-contractors are aware of the confidential nature of the Confidential Information subject to any such agents and sub-contractors providing the Service Provider with an undertaking to keep the Confidential Information disclosed to it confidential in similar terms to the provisions of this **clause 28.5**.

29.2 The obligations set out in **clause 29.1** shall not apply to any Confidential Information which:

29.2.1 the Service Provider can show by documentary evidence was already in its lawful possession and at its free disposal otherwise

than directly or indirectly from the Authority or any other TfL Group Member;

29.2.2 is lawfully disclosed to the Service Provider without any obligations of confidence, by any person who has not derived it directly or indirectly from the Authority or any other TfL Group Member;

29.2.3 is or has come into the public domain through no fault of the Service Provider or its personnel;

29.2.4 is required by law or by order of a court of competent jurisdiction to be disclosed but only to the extent required by such law or order;

29.2.5 is disclosed with the prior written consent of the Authority; or

29.2.6 is disclosed pursuant to **clause 29.7**.

29.3 The Service Provider acknowledges that damages would not be an adequate remedy for any breach of **clause 29** and that (without prejudice to all other rights, powers and remedies which the Authority may be entitled to as a matter of law) the Authority shall be entitled to seek the remedies of injunction, specific performance and other equitable relief to enforce the provisions of this **clause 29** and no proof of special damages shall be necessary for the enforcement of the provisions of this **clause 29**.

29.4 The Service Provider's obligation of confidentiality in this **clause 29** shall survive the termination of this Agreement.

29.5 For the avoidance of doubt, **clause 29.7** shall take precedence over this **clause 29.5** to the extent of any inconsistency.

29.6 The Service Provider acknowledges that the Authority is subject to the Transparency Commitment. Accordingly, notwithstanding any other provision of this Agreement, the Service Provider hereby gives its consent for the Authority to publish the Contract Information to the general public.

29.7 The Authority may in its absolute discretion redact all or part of the Contract Information prior to its publication. In so doing and in its absolute discretion

the Authority may take account of the exemptions/exceptions that would be available in relation to information requested under the FOI Legislation. The Authority may in its absolute discretion consult with the Service Provider regarding any redactions to the Contract Information to be published pursuant to **clause 29.6**. The Authority shall make the final decision regarding publication and/or redaction of the Contract Information.

30. **FREEDOM OF INFORMATION**

30.1 The Service Provider acknowledges that the Authority:

30.1.1 is subject to the FOI Legislation and agrees to assist and co-operate with the Authority to enable the Authority to comply with its obligations under the FOI Legislation; and

30.1.2 may be obliged under the FOI Legislation to disclose Information without consulting or obtaining consent from the Service Provider and, subject to the provisions of this **clause 30**, may ultimately at its discretion disclose such Information.

30.2 Without prejudice to the generality of **clause 30.1**, the Service Provider shall and shall procure that its sub-contractors (if any) shall:

30.2.1 transfer to the Authority each Information Request relevant to this Agreement, the Services, the Software or any TfL Group Member that it or they (as the case may be) receive as soon as practicable and in any event within two (2) Business Days of receiving such Information Request; and

30.2.2 in relation to Information held by the Service Provider on behalf of the Authority, provide the Authority with details about and/or copies of all such Information that the Authority requests and such details and/or copies shall be provided within five (5) Business Days of a request from the Authority (or such other period as the Authority may reasonably specify) and in such forms as the Authority may reasonably specify.

30.3   The Authority shall be responsible for determining whether Information is exempt information under the FOI Legislation and for determining what Information will be disclosed in response to an Information Request in accordance with the FOI Legislation. The Service Provider shall not itself respond to any person making an Information Request, save to acknowledge receipt, unless expressly authorised to do so by the Authority.

30.4   This **clause 30** shall survive termination of this Agreement.

31.   **DATA PROTECTION**

31.1   The Service Provider shall comply with all of its obligations under the DPA and, if Processing Personal Data on behalf of the TfL Group (**"Authority Personal Data"**), shall only carry out such Processing for the purposes of providing the Services and the Software in accordance with this Agreement and in accordance with any obligations imposed by the Authority in **Schedule 1** and any other instructions from the Authority as may be specified from time to time.

31.2   Without prejudice to the generality of **clause 31.1**, the Service Provider shall:

31.2.1   take appropriate technical and organisational security measures, that are satisfactory to the Authority, against unauthorised or unlawful Processing of Authority Personal Data and against accidental loss, destruction of, or damage to such Personal Data;

31.2.2   provide the Authority with such information as it may from time to time require to satisfy itself of compliance by the Service Provider with **clause 31.2.1**;

31.2.3   co-operate with the Authority in complying with any subject access request made by any Data Subject pursuant to the DPA and/or responding to any enquiry made or investigation or assessment of Processing initiated by the Information Commissioner in respect of any Authority Personal Data;

31.2.4 when notified by the Authority, comply with any agreement between the Authority and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Authority Personal Data;

31.2.5 take reasonable steps to ensure the reliability of Personnel having access to Authority Personal Data and to ensure that such Personnel are fully aware of the measures to be taken and the Service Provider's obligations under this **clause 31.2.5** when Processing Authority Personal Data; and

31.2.6 not Process any Authority Personal Data outside the European Economic Area (or any country deemed adequate by the Commission pursuant to Article 25(6) Directive 95/46/EC) without the TfL Group's prior written consent and, in the event of such consent, only if the Service Provider has agreed in writing to reasonable provisions imposed by the Authority relating to such Processing.

31.3 When the Service Provider receives a written request from the Authority for information about, or a copy of, Authority Personal Data, the Service Provider shall supply such information or data to the Authority within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within ten (10) Business Days from the date of the request.

31.4 The Authority remains solely responsible for determining the purposes and manner in which Authority Personal Data is to be Processed. The Service Provider shall not share any Authority Personal Data with any sub-contractor or third party unless there is a written contract in place between the Service Provider and sub-contractor or third party which requires the sub-contractor or third party:

31.4.1 to only Process Authority Personal Data in accordance with the TfL Group's instructions to the Service Provider; and

31.4.2 to comply with the same obligations with which the Service Provider is required to comply under this **clause 31**.

31.5 This **clause 31** shall survive termination of this Agreement.

32. **AMENDMENT AND WAIVER**

32.1 This Agreement may only be varied or amended with the written agreement of both parties. The details of any variations or amendments shall be set out in such form as the Authority may require and which may be substantially in the form set out in **Schedule 7** and shall not be binding upon the parties unless completed in accordance with such form of variation.

32.2 Any waiver of a breach of any of the terms of this Agreement shall not be deemed a waiver of any subsequent breach and shall not affect the other terms of this Agreement.

33. **EMPLOYEES**

33.1 Nothing in this Agreement will render the Service Provider's Personnel an employee, agent or partner of the Authority or of any member of the TfL Group by virtue of the provision of the Services by the Service Provider under this Agreement and the Service Provider shall be responsible for making appropriate deductions for tax and national insurance contributions from the remuneration paid to the Service Provider's Personnel.

33.2 Notwithstanding **clause 33.1**, the Service Provider shall indemnify, keep indemnified and hold harmless the TfL Group from and against all liabilities, costs, expenses, injuries, direct or indirect or consequential loss, damages, claims, demands, proceedings and legal costs (on a full indemnity basis) which the Authority or the TfL Group incur or suffer whenever arising or brought by the Service Provider's Personnel or any person who may allege to be the same.

33.3 The Service Provider shall pay to the Service Provider's Personnel not less than the amounts declared to the Authority (if any) as part of the tender process for this Agreement and not less than the amounts to which the Service Provider's Personnel are contractually entitled.

33.4   *NON-SOLICITATION*

33.4.1 Subject to **clause 33.4.2**, neither the Service Provider nor the Authority shall, whether directly or indirectly and whether alone or in conjunction with, or on behalf of, any other person and whether as a principal, shareholder, director, employee, agent, consultant, contractor or otherwise:

at any time during the Term solicit, induce or entice away or endeavour to solicit, induce or entice away from the other party any person employed by or contracted to that party in a senior and/or skilled capacity where such person is engaged at any time during the term in the performance of this Agreement whether or not such person would commit any breach of his or her contract of employment or engagement by leaving the employment or engagement of the other party;

at any time during the Term employ, engage or appoint any person employed by the other party in any senior and/or skilled capacity where such person is engaged at any time during the term in the performance of this Agreement and where such person would commit a breach of his or her contract of employment by leaving the employment of the other party;

at any time during the period of twelve (12) months following the end of the Term, solicit, induce or entice away or endeavour to solicit, induce or entice away, from the other party any person employed by or contracted to the other party in a senior and/or skilled capacity where such person was engaged at any time during the final three (3) months of the term in the performance of this Agreement (including employees whose employment has transferred to the Authority or a new service

provider pursuant to the Transfer of Undertakings (Protection of Employment) Regulations 2006 after the end of the Term) whether or not such person would commit any breach of his or her contract of employment or engagement by leaving the employment or engagement of the other party; or

at any time during the period of twelve (12) months following the end of the Term employ, engage or appoint any person employed by the other party in a senior and/or skilled capacity where such person was engaged at any time during the final three (3) months of the term of this Agreement in the performance of this Agreement and where such person would commit a breach of his or her contract of employment by leaving the employment of the other party.

33.4.2 This **clause 33.4** shall not prevent employment resulting from general recruitment advertising which shall not constitute a breach of **clause 33.4**.

33.5 Subject to **Schedule 1**, the parties confirm that the Transfer of Undertakings (Protection of Employment) Regulations 2006 are not envisaged to apply on the Commencement Date or the termination of this Agreement.

33.6 This **clause 33** shall survive termination of this Agreement.

34. **NOTICES**

34.1 Any notice, demand or communication in connection with this Agreement will be in writing and may be delivered by hand, prepaid recorded delivery first class post or facsimile addressed to the addressee at the address stated in **Schedule 1** (or in the absence of such address being set out, the recipient's registered office), or any other address and facsimile number notified to the other party in writing in accordance with this clause as an address to which

notices, demands and communications may be sent. The notice, demand or communication will be deemed to have been duly served:

34.1.1   if delivered by hand, at the commencement of the following Business Day;

34.1.2   if delivered by post, seventy-two (72) hours after being posted or, in the case of airmail, ten (10) Business Days after being posted; or

34.1.3   if delivered by facsimile, at the commencement of the following Business Day, provided that a confirming copy is sent by first class post to the other party within twenty-four (24) hours after transmission.

35.   **PUBLICITY**

35.1   Subject always to the provisions of **clause 35.3**, no announcement, circular, advertisement or other publicity (including any communication with representatives of the general or technical press, radio, television or other communications media) in connection with this Agreement, its subject matter or any ancillary matter will be made or issued by or on behalf of the Service Provider without the prior written consent of the Authority. The Authority shall have the right to approve any such announcement, circular, advertisement or other publicity before it is made.

35.2   The Service Provider agrees and shall ensure that the Authority has the right to control and to supervise all dealings with the press and any other media in relation to any incident, event, claim or action arising in connection with this Agreement.

35.3   Without prejudice to the generality of the foregoing, the Service Provider shall not (without the prior written approval of the London Organising Committee of the Olympic Games Limited (**"LOCOG"**) in each case) represent that any products or services provided under this Agreement have been endorsed or approved by the Authority, the British Olympic Association, the British Paralympic Association, LOCOG or any other official Olympic or Paralympic body, or that the Service Provider (including any of its products or services)

are in any way associated with those organisations, the Olympic Games and/or Paralympic Games, or London 2012, including by publishing or issuing any statement (factual or otherwise) about the Service Provider's provision of the products or services under this Agreement.

36. **DISASTER RECOVERY**

36.1 The Service Provider will ensure at all times it has in place a Disaster Recovery Plan and that the Disaster Recovery Plan is adequate to minimise the effect of any Disaster.

36.2 Unless the Disaster was caused by a Force Majeure Event which a reasonable disaster recovery plan would not be expected to protect against, the Service Provider's liability to pay the Service Credits will continue to accrue until such time as the Services are performed by the Service Provider in accordance with the provisions of this Agreement and the Service Levels. Without prejudice to the generality of the foregoing, a reasonable disaster plan should protect against incidents involving fire, interruption in power supply, act of terrorism, threat of act of terrorism, earthquake, extraordinary storm, flood or abnormal weather conditions.

36.3 In the event of a Disaster, the Service Provider will immediately implement the Disaster Recovery Plan and will continue to provide those Services which are not affected by the Disaster in accordance with the provisions of this Agreement. In respect of any part of the Services which are affected by the Disaster, the Service Provider will comply with the Disaster Recovery Plan, the rest of this **clause 36** and this Agreement.

36.4 Not used

37. **INDEMNITY - CONDUCT OF CLAIMS**

37.1 In respect of any claim arising under any indemnity contained in this Agreement, the party indemnified (**"indemnified party"**) will:

37.1.1 as soon as possible give to the party giving the indemnity (**"indemnifying party"**) written notice of the claim, circumstance or matter against which that party is claiming to be indemnified, and all

details of the claim from time to time in the knowledge or possession of that party;

37.1.2 where the claim relates to a claim by any third party against that party, not without the prior written consent of the other party (which will not be unreasonably withheld or delayed) admit liability or make any offer, promise, compromise, settlement or communication with the third party in respect of the claim; and

37.1.3 where the claim is by a third party against the indemnified party,

at the request of the indemnifying party; and

provided at all times that the indemnifying party provides to the reasonable satisfaction of the indemnified party security for all costs, charges and expenses,

surrender to the indemnifying party or its insurers the conduct, in the indemnified party's name, of the defence, settlement and/or counterclaim to the third party's claim (provided that the indemnified party will be kept fully informed as to the conduct of such defence, settlement and/or counterclaim).

38. **LAW AND DISPUTE RESOLUTION**

38.1 The formation, existence, construction, performance, validity and all aspects whatsoever of this Agreement or of any term of this Agreement as well as any non-contractual obligations arising out of or in connection with it shall be governed by English law. The English courts shall have exclusive jurisdiction to settle any disputes which may arise out of or in connection with this Agreement. The parties agree irrevocably to submit to that jurisdiction.

38.2 If the Dispute is not settled through discussion between the representatives of the parties within a period of seven (7) Business Days of the date on which the Dispute arose, the parties may refer the Dispute in writing to a director or chief executive (or equivalent) (**"Senior Personnel"**) of each of the parties for resolution.

38.3   If the Dispute is not resolved within ten (10) Business Days of referral to the Senior Personnel, either party may propose by notice to the other party (**"Notice"**) that a structured mediation or negotiation be entered into with the assistance of a mediator.

38.4   If, within twenty (20) Business Days of the service of the Notice, the parties are unable to agree on a mediator or if the agreed mediator is unable or unwilling to act, either party may apply to the Centre for Effective Dispute Resolution (**"CEDR"**) in London to appoint a mediator. The costs of that mediator shall be divided equally between the parties or as the parties may otherwise agree in writing.

38.5   Where a dispute is referred to mediation under **clause 38.4**, the parties will attempt to settle such Dispute by mediation in accordance with the model mediation procedures published by CEDR or such other procedures as the mediator may recommend.

38.6   If the parties reach agreement on the resolution of the Dispute, such agreement shall be recorded in writing and once signed by the parties' authorised representatives, shall be final and binding on the parties.

38.7   If either party refuses at any time to participate in the mediation procedure or in any event if the parties fail to reach agreement on the Dispute within forty (40) Business Days of the service of the Notice either party may commence proceedings in accordance with **clause 38**.

38.8   For the avoidance of doubt, the Service Provider shall continue to perform its obligations under this Agreement in accordance with this Agreement and without delay or disruption while the Dispute is being resolved pursuant to this **clause 38**.

38.9   Neither party shall be prevented from, or delayed in, seeking any order for specific performance or for interim or final injunctive relief as a result of the provisions of this **clause 38**.

39.   **RIGHTS OF THIRD PARTIES**

39.1   Save that any TfL Group Member has the right to enforce the terms of this Agreement in accordance with the Contracts (Rights of Third Parties) Act 1999 (**"Third Party Act"**), the parties do not intend that any of the terms of this Agreement will be enforceable by virtue of the Third Party Act by any person not a party to it.

39.2   Notwithstanding **clause 39.1**, the parties are entitled to waive time, vary or rescind this Agreement without the consent of any TfL Group Members.

40.   **ENTIRE AGREEMENT/RELIANCE ON REPRESENTATIONS**

40.1   This Agreement and the documents and Schedules and Annexes which are incorporated into and form part of this Agreement contain all the terms which the parties have agreed in relation to the subject matter of this Agreement and supersede any prior written or oral agreements, representations or understandings between the parties in relation to such subject matter.

40.2   The Service Provider acknowledges that this Agreement has not been entered into wholly or partly in reliance on, nor has the Service Provider been given, any warranty, statement, promise or representation made by or on behalf of the Authority other than as expressly set out in this Agreement. To the extent that any such warranties, statements, promises or representations have been given the Service Provider unconditionally and irrevocably waives any claims, rights or remedies which it might otherwise have had in relation to them.

40.3   Nothing in this **clause 40** will exclude any liability which one party would otherwise have to the other party in respect of any statements made fraudulently.

41.   **GENERAL**

41.1   Nothing contained in this Agreement, and no action taken by the parties pursuant to this Agreement, will be deemed to constitute a relationship between the parties of partnership, joint venture, principal and agent or employer and employee. Neither party has, nor may it represent that it has, any authority to act or make any commitments on the other party's behalf.

41.2   The failure or delay by either party to this Agreement in exercising any right, power or remedy of that party under this Agreement shall not in any circumstances impair such right, power or remedy nor operate as a waiver of it.   The single or partial exercise by either party to this Agreement of any right, power or remedy under this Agreement shall not in any circumstances preclude any other or further exercise of it or the exercise of any other right, power or remedy.

41.3   This Agreement may be executed in any number of counterparts or duplicates, each of which shall be an original, and such counterparts or duplicates shall together constitute one and the same agreement.

SCHEDULE 1

Key Contract Information

Service Provider
Arqiva Limited a *company* registered in England and Wales with registration number 02487597 and whose *registered* office is at Crawley Court, Crawley, Winchester, Hampshire, SO21 2QA

the TfL Group
TfL and all of its subsidiaries (as defined in Sections 736 and 736A of the Companies Act 1985), which definition shall include the Authority (whether or not the Authority is a subsidiary and reference to any **"TfL Group Member"** shall refer to TfL, the Authority and/or any such company, as applicable

Agreement End Date
10 years with negotiated break points at fixed intervals of 5+3+2

Business Hours
24 hours, 7 days a week, 365 (366 on leap years) days a year

Service Provider's Equipment
Not applicable

Key Personnel (Service Provider's)
REDACTED

Site
Palestra, 197 Blackfriars Road, London, SE1 8NJ

Warranty Period(s)
6 months from Acceptance in respect of each element of the Software and 6 months in respect of the whole Software

	upon completion and final acceptance
Euro Compliance Required?	No
Time period for payment under clause 4.5 (if different to the 30 day period set out in clause 4.5)	30 days from the Authority's receipt of invoice
Force Majeure Period	a period being no more than **30** days after the first date of the applicable Force Majeure Event
Insurances	See Insurances Annex in this **Schedule 1**
Level for clause 18.2.8, if different to £100,000	Not Applicable
Service Provider's IPR, including any Service Provider Software	Not Applicable
Third Party IPR, including any Third Party Software:	All Intellectual Property Rights in the Software and Services which are owned by the third party EXCEPT:
	REDACTED

Details of Software Licences for Third Party Software and which party is going to procure them	REDACTED
	READCTED
Details of agreed back-ups to be provided by the Service Provider in respect of the Data and Software, if any, and intervals in which they are to be performed	Not applicable
Disaster Recovery	If the Authority requires to specify details of, or approve the Service Provider's Disaster Recovery Plan, then insert detail here. This may be particularly applicable to any Maintenance Services. To be discussed
Are the Services or Software for business critical or safety critical parts of the TfL Group, its estate or services or otherwise Services or Software which require continuous uninterrupted service?	No
Liquidated Damages	REDACTED

Liquidated Damages Period: REDACTED

Reports to be provided other than or in addition to those set out under clause 16.7

Subject to Schedule 2 Annex B

Dates for production of reports under clause 16.7 if more or less than monthly

Reports are required each period (a period is 4 weeks) unless otherwise agreed

Notice Period for Termination for Convenience in accordance with clause 23.8

90 days

Service Provider's Liability Cap

REDACTED

REDACTED

REDACTED

The TfL Group's Liability Cap   REDACTED

Data Protection   N/A

Address to send the Authority Notices to   For attention of Fardeen Moorudun

3rd Floor, Petty France, Room 391/392,

	55 Broadway, London, SW1H 0BD
	Copy to
	General Counsel
	6th Floor, Windsor House, 50 Victoria Street, London, SW1H 0TL
	Facsimile Number: 020 7126 4598
Address to send Service Provider Notices to	For attention of: Group Commercial Director
	REDACTED
Escrow/Verification Provisions	Required by the Authority Yes,Upon request.
	Detail of services required:
	Escrow: Yes
	Verification ServicesYes – to be verified by the Escrow provider on receipt of material
	Cost to be borne by TfL

Agreed Equality Policy required?	No
Authority Address where invoices are to be submitted to	Accounts Receivable, 14 Pier Walk, London, SE10 0ES
Electronic format required (if any) for submission of orders by the Authority and of invoices by the Service Provider	No

ANNEX A

INSURANCES

1.   Insurance to be held by Service Provider in accordance with **clause 18**:

    (a)   Employer's liability insurance in respect of the Service Provider's liability for death, personal injury or occupational disease of any person in the Service Provider's employment in the sum of not less than five million pounds (£5,000,000) per incident or such other minimum level as may from time to time be required by law;

    (b)   Public liability insurance in respect of the Service Provider's liability for loss or damage to property (including property of the Authority or for which it is responsible), and against liability for death, injury or occupational disease in the sum of not less than five million pounds (£5,000,000) per occurrence and shall be endorsed to provide that no act or omission on the part of the Service Provider shall prejudice the TfL Group's rights under such policy as principal;

    (c)   Professional indemnity insurance in a sum normal and customary for a Service Provider in the business of providing services of a similar scope, nature and complexity to the Services but not less than five hundred thousand pounds (£500k) in the aggregate per annum for the Term and for six (6) years after expiry or termination of this Agreement; and

ANNEX B

SPECIAL CONDITIONS OF CONTRACT

Not applicable

SCHEDULE 2

Services

SAFE Software

Additionally, the Software shall be supplied in accordance with the Provision of Software Annex set out in this **Schedule 2**.

Maintenance Services

Software in respect of which Maintenance Services are being provided: SAFE Software

Maintenance Services Commencement Date: **Go Live**

The Software shall be maintained in accordance with the Maintenance Services Annex set out in this **Schedule 2**.

Additional Services

Description of Additional Services: Not Applicable

Training Service:

System Administrators training

System Administrator training parts

- SAFE System fundamentals
- SAFE Workflow and Configuration
- SAFE GIS basics and GIS maintenance
- System Basic and Advanced Administration
- System Maintenance
- SAFE Database Schema and Reports interface

Duration: 2 days – Assumes TfL Location in London

Train the Trainer training

Train the Trainer parts

- SAFE System fundamentals
- SAFE Workflow and Configuration
- SAFE Incident Management
- SAFE GIS
- SAFE Mobile
- SAFE Basic Administration

Duration: 3 days - Assumes TfL Location in London

Additionally, the Additional Services Annex set out in this **Schedule 2** shall apply to Additional Services.

ANNEX A

PROVISION OF SOFTWARE

1. **SOFTWARE**

1.1 **RISK**

Risk in the media on which the Software is recorded shall pass to the Authority on delivery of such media to the Authority or Acceptance of the Software (whichever is the latter).

1.2 **LICENCE(S)**

Prior to commencing work on building the Software and procuring and developing the Software, the Service Provider shall specifically identify any applicable

Third Party Software intended for supply, agreeing with the Authority in advance (at the TfL Group's option) whether the Authority or the Service Provider is to obtain the licences necessary to use such Third Party Software and the terms upon which such licence should be granted to use such Third Party Software and, where the Service Provider procures such licence, it will agree with the Authority the terms upon which such licence should be granted, in so far as it is able to do so with the Third Party Software provider.

PROVISION OF SOFTWARE

The Software shall be provided to the Authority in accordance with this Agreement and the relevant Project Plan.

ANNEX B

MAINTENANCE SERVICES

For the purposes of this **Annex** the following expressions will have the following meanings unless inconsistent with the context:

"Availability"	An ITIL term means the ability of the Software and associated services provided by the Service Provider, to perform its agreed function when required
"Availability Target"	means the target against which the Availability of the Software is measured in accordance with paragraph 15.3
"Configuration Item" or **"CI"**	means a component or an element of a component of the Software
"Configuration Management"	means the ITIL process of identifying and defining Configuration Items in a system, recording and reporting the status of Configuration Items and Requests for Change, and verifying the completeness and correctness of Configuration Items
"Consultancy Day"	means provision of a resource (as may be specified in **Schedule 3**) by the Service Provider for one Business Day
"Contract Year"	means the twelve (12) months starting on the day of Go Live and each subsequent anniversary of such date for the duration of the term of this Agreement
"Critical Application"	means any application(s), software, equipment or service which the Authority considers are critical

applications for the purposes of allocating priorities under paragraph 4.1 of this **Annex B** of **Schedule 2**

"Fault"   means a single root cause event that leads to one or more functional components of the Software not conforming to their Specification or operating manual

"Go Live"   means the date on which the Authority places the Software into live operation other than for testing purposes

"Implementation"   means the act of upgrading the Live Environment to affect a Release

"Incident"   any event which is not part of the standard operation of the Software which causes, or may cause an interruption to or reduction in the quality of the Software. For the avoidance of doubt, this shall include unplanned outages. In this Agreement, an Incident can be either a **"Software Error"** or a **"Fault"**

"ITIL"   means Information Technology Infrastructure Library. This is a methodology or framework to set out the best practice for delivery of IT services

"Known Error"   means a Problem or potential Problem when the cause becomes understood, and where an Incident is raised which is a manifestation of it and has a Workaround

"Live Environment"   means those aspects of the Services that constitute the operational environment for the TfL Group Users

"Major Adjustment"	means a modification to the Software requested by the Authority (other than a modification made necessary or desirable as a result of a Problem or an Incident) which is estimated by the Service Provider to be greater than [twenty (20) Man Days' effort]
"Major Incident"	means Incidents categorised as Severity 1 or Severity 2 in paragraph 4 of this **Annex B** of **Schedule 2**
"Major Incident Report"	means a report produced following a Major Incident giving a description of the Incident, details of the reasons for the Incident, and rectification plans implemented to ensure the Incident is not repeated
"Man Day"	means the effort done by one person during or equivalent to 8 hours
"Man Hour"	means the effort done by one person during one hour or a combination of persons and hours to provide an equivalent effort (for example, 12 man hours is the effort done by one person during 12 hours or by two persons during 6 hours or by three persons during 4 hours, and so on)
"Measurement Period"	means the Authority's financial periods (4 weeks) as provided to the Service Provider from time to time
"Operational Level Agreement"	means a definition of the relationship and the interactions between the Service Provider and the Primary Service Provider to support the overall achievement of the Service Levels
"Periodic Service Report"	means a report to be provided by the Service

Provider showing the achievement and trends against Service Levels. The frequency and content is set out in paragraph 9 of this Annex B of Schedule 2.

"Persistent Breach" means when one or more of the criteria specified under paragraph **21.1** of this Schedule 2 are fulfilled

"Primary Service Desk" means the service desk provided by the Primary Service Provider – this service is available 24 x 7, three hundred and sixty-five (365) days per year

"Primary Support Hours" **means 24 hours a day, 7 days a week, 365/6 days a year.**

"Primary Service Provider" or "PSP" means the TfL Group's provider(s) of core services including but not restricted to: service desk; desktop support and LAN as more particularly described in paragraph 14.2 of this **Annex B** of **Schedule 2**

"Problem" **an ITIL term meaning** the underlying cause of one or more Incidents.

"Problem Management" The ITIL Process responsible for managing the lifecycle of all Problems.

"Problem Rectification Plan" means a plan to implement a permanent fix to a Problem, including any proposed changes to CIs, testing of the proposed fix(es) and plans for Release into the Live Environment

"Quarter" means any successive period of three (3) calendar months measured from the start of the first Contract Year

"Release" means a collection of new and/or changed CIs

	which are tested and introduced into the Live Environment together
"Release Management"	means the ITIL process describing how Releases are managed
"Release Note"	means a short document summarising the details of an individual Release. It includes a list of CIs that form the Release
"Request for Change" or **"RFC"**	means a form, possibly electronic, used to record the details of any request for a change to the CIs or other aspects of the Software
"Resolution (Incident)"	means action that will result in the resumption of service and the removal or negation of the effect of an Incident
"Resolution (Problem)"	means action that will result in the removal of a Problem and normally the permanent fixing of one or more Incidents, removing the need for associated Workarounds
"Resolve"	means the act of supplying Resolution of an Incident or Problem
"Resolver Group"	means the function of the Service Provider assigned to investigate Incidents and propose Resolution
"Response"	means the first contact back to the TfL Group User subsequent to contacting the Service Desk to raise an Incident and **"Respond"** shall be construed accordingly. This response is to be made by a suitably knowledgeable Resolver Group which may be the Service Desk itself during

	the same contact as the raising of the Incident
"Restoration"	means action that will result in the resumption of service without the removal of the cause of an Incident. This may be a Workaround and does not necessarily mean that the underlying cause is rectified
"Restore"	means the act of supplying Restoration to an Incident or Problem
"Root Cause"	an ITIL term meaning the underlying or original cause of an Incident or Problem.
"Root Cause Analysis"	an ITIL term referring to activity that identifies the Root Cause of an Incident or Problem.
"Secondary Support Hours"	means 08:00 – 18:00, Monday to Friday excluding bank holidays.
"Service Credit Percentage"	means the percentages set out under paragraph **20.3** of this **Schedule 2 Annex B**
"Service Desk"	means the Service Provider's single point of contact for logging, resolving and management of all requests for support by the TfL Group Users and the PSP
"Severity Level"	means the level of severity assigned to an Incident or Fault as described under paragraph **4.1** of this **Schedule 2, Annex B**
"Small Functional Adjustment"	means a modification to the Software requested by the Authority which is estimated by the Service Provider to be less than [twenty (20) Man Days effort] to build, test and deploy
"Software Error"	means any non-compliance by the Software with

the features and functionalities set forth in the documentation supplied for the version, causing reproducible errors in the operation of the Software

"Software Support" means Software Error correction (corrective maintenance), technical advice, training, coaching, providing clarifications by telephone, fax, e-mail, and on site at the TfL Group's premises, to solve any problems that may arise concerning the operation of the Software

"Support Hours" means the hours during which support will be rendered by the Service Provider to the Authority which shall be either the Primary Support Hours or Secondary Support Hours as specified in section 5.2 and 5.3 of this schedule

"TfL Group User" means those TfL Group persons using the Software

"Version" means a baseline of a Configuration Item which has significant added functionality to its predecessor

"Workaround" means a solution to an Incident or a Problem that does not involve rectifying the underlying cause but rather relies on an alternative method of usage

References in this **Annex B** of **Schedule 2** and to a **"paragraph"** shall mean a paragraph to this **Annex B** of **Schedule 2** and a reference to a **"clause"** shall mean a clause in the main body of the Agreement unless otherwise specified or inconsistent with the context.

1.1.1. **1.   Maintenance Services**

1.1   The Service Provider agrees to provide the following Maintenance Services to the Authority during Support Hours in respect of the Software:

1.1.1   reasonable assistance in the resolution of Incidents and Problems via a telephone call originated by the Authority;

1.1.2   recommendations relevant to the course of action necessary to recover from a fault, error or failure emanating from the Software or its use;

1.1.3   replacement of a tangible Copy of the Software where that Copy has been accidentally damaged, upon return of the damaged Copy to the Service Provider at no charge other than the Service Provider's current packaging and shipping charges and the Service Provider's current charge for the media upon which the replacement Copy is provided;

1.1.4   upon request by the Authority, the diagnosis of Faults in the Software and the rectification of such Faults (remotely or by attendance at the TfL Group's premises) by the issue of fixes or other such remedy in respect of the Software;

1.1.5   the creation and dispatch to the Authority from time to time of fixes in respect of the Software; and

1.1.6   the creation and dispatch to the Authority from time to time of new Versions and Releases of the Software.

1.2   The Maintenance Services may be performed at one of the Service Provider's premises or via an approved network link or at the TfL Group's Premises. In the event of a modem being utilised the Authority shall at the Service Provider's request initiate the telephone call. If possible, the Authority shall provide access to and copies of such test data as the Service Provider may reasonably require for the performance of the Maintenance Services. Except for the Service Provider's Personnel engaged in the performance of the Services, the Service Provider shall not disclose such of the information as is contained in the data and which can reasonably be regarded by the Service Provider to be secret and confidential to a Third Party for so long as the same

is secret and confidential. The Authority shall provide the Service Provider with reasonable access to the Software during Business Hours to enable the Service Provider to comply with its obligations under this **Annex B** of **Schedule 2**.

1.3 The Charges shall include the provision and implementation of the diagnosis and rectification of a Fault arising in the following Versions of the Software:

    1.3.1 the then current Version supplied by the Service Provider to the Authority; and

    1.3.2 the Versions which were supplied by the Service Provider to the Authority but have been superseded by the latest Version within the period of two years ending on the date of the request for such diagnosis and rectification by the Service Provider.

The Service Provider will provide diagnosis and rectification services in respect of other Versions as Additional Services.

1.1.2. **2.   Fault Categorisations and Corrections**

2.1   Error Correction

    2.1.1 The Service Provider will maintain the Software in such working order as enables it to perform the functions specified in the Specification and the user manuals.

    2.1.2 The Authority will notify the Service Provider of any Fault, and provide the Service Provider (in so far as the Authority is reasonably able) with a documented example of the Fault and a description of and the circumstances in which the Fault arose within a reasonable time of becoming aware of such circumstances.

    2.1.3 On receipt of a request for correction of any Fault reported by the Authority or identification by the Service Provider of such Fault, the Service Provider will ensure that an appropriately qualified and experienced person commences investigatory and corrective work within the response time specified in paragraph 5 below applicable to

the category into which the reported Fault falls. If the reported Fault is either Severity 1 or 2 (as set out below) the Service Provider will diligently continue investigatory and remedial work throughout the Support Hours or such other times as may be mutually agreed between the parties until the reported Incident or Problem has been Restored. Findings from investigatory/remedial work will be fed back to the Authority.

2.1.4 Upon the Fault being Restored the Service Provider will supply to the Authority the corrected version of the object code of the Software in machine-readable form for loading into the Live Environment. As soon as reasonably practicable after that the Service Provider will supply the Authority with amendments to the Documentation specifying the nature of the correction and providing instructions for the use of the corrected version of the Software where appropriate.

2.1.5 If requested by the Authority the Service Provider will provide, as soon as reasonably practicable, training for designated members of the TfL Group's staff to enable the Authority to make proper use of the corrected version of the Software. Where applicable, the Service Provider will in addition provide the Authority with such assistance as is reasonably necessary to enable the Authority to implement the use of the corrected version of the Software. For the avoidance of doubt, the provision of such training and assistance is included within the Charges, and excludes travel expenses and the Service Provider shall not be entitled to any additional payments in respect of such training.

2.1.6 The Service Provider will notify the Authority promptly of any significant fixes, patches or Workarounds in respect of the Software which are available to correct Faults identified by the Service Provider or the Authority users together with details of any material effects which such fixes, patches or Workarounds may be expected to have.

1.1.3. **3.   Fault Reporting**

3.1   Requests for Support

3.1.1   The Service Provider shall provide a Service Desk and single telephone number through which Support shall be requested. The Authority may request Support by telephone, fax, e-mail (if practicable) or letter, as appropriate to the situation. The TfL Group's staff will contact the TfL Group's Primary Service Desk in the first instance for Support, and if further Support is required, the TfL Group's Primary Service Desk personnel will contact the Service Provider.

3.1.2   The Service Provider shall log all requests for Support, including:

(a)   the date and time of the request;

(b)   how received (telephone, fax, e-mail, letter);

(c)   the name of the person making the request;

(d)   the nature of the request (subject matter); and

(e)   the severity of the request, as specified by the Authority.

3.1.3   The Service Provider shall assign a unique log number to each request and notify this number to the Authority at the time the request is made. This number shall then be used in all follow-up actions and reporting.

3.2   The Service Provider shall maintain an accurate and up to date record of all Faults reported, showing the date and time of Fault, nature of the Fault, actions taken, status, expected or actual resolution time and shall provide the same to the Authority upon request.

1.1.4. **4.   Assignment of Priorities**

4.1   The Severity Level of the request shall be determined by the Authority, in accordance with the following scale:

Severity 1: a) All or any part of the Critical Applications are unavailable which may result in the failure of business critical activities; and/or

(b) A service or application failure which affects over fifty percent (50%) of potential TfL Group Users of that service or application within a business unit of the Authority; and/or

(c) Incidents reported that in the opinion of the Authority have a high business impact on business-critical units of the Authority; and/or

(d) Any other incident falling outside (a) (b) or (c) occurs and such failure, in the TfL Group's opinion, affects the security of the TfL Group's infrastructure or has a detrimental impact on the information management (**"IM"**) operations of the Authority or, in either case, such failure is in the TfL Group's opinion likely to do so.

Severity 2: Business processes are adversely affected resulting in some impact in business operations that do not fall within the scope of Severity Level 1 and:

(a) The Incident has impacted one or more of the TfL Group's business units such that one or more business functions are affected; and either

(b) The Incident affects four (4) or more Users, or shared functions are unavailable (e.g. for the purposes of illustration only, switch or server repairs); or

(c) The Incident causes a failure of redundant services which increases the risk to the Critical Applications.

Severity 3: TfL Group business processes are adversely affected resulting in some impact in business operations that do not fall within the scope of Severity Level 1 or Severity Level 2, which includes where:

(a) All or part of the applications, software or services are adversely affected, but the impact is on less than four (4) TfL Group Users; and/or

(b) The Incident prevents TfL Group Users from effectively performing business activities and, although important, the TfL Group's business units' key business activities are not adversely affected; and/or

(c) The Incident is limited in scope and scale. This includes equipment failures where, due to redundancy and resilience, TfL Group User service is unaffected; and/or

(d) An enquiry where there is no actual loss of service to the Authority User, but rather a simple need for information that does not require a request for information (**"RFI"**).

Severity 4: All other requests for service where there is no Incident or problem.

4.2 The initial classification of severity is to be made by the Authority and will be confirmed on receipt by the Service Provider. In the event of any disagreement in the classification relating to Severity 1 or 2 reports, this will be escalated by the Service Provider's Programme Manager with his relevant counterpart in the Authority so as to minimise any delay in Response, Restore and Resolve times. While under escalation and until resolved, the Service Provider will perform the Maintenance Services in accordance with the Severity Level set by the Authority.

1.1.5. **5.   Response and Resolution Times**

5.1 From the time when a request is received by the Service Provider from the PSP, the Service Provider shall Respond within the following timeframes:

Severity	Response	Incident Restore	Incident Resolve
1	15 minutes	See Achievement , Measure column in section 5.2	See section 5.2
2	45 minutes	See Achievement Measure column in	See section 5.2

		section 5.2	
3	3 hours	See Achievement Measure column in Section 5.2	See section 5.2
4	1 Business Day	See Achievement Measure column in Section 5.2	See section 5.2

For the duration of the Fault Resolution, the originator of the request shall be advised of progress as follows:

(a) Severity 1 - every thirty (30) minutes during Support Hours or such other times as may be mutually agreed.

(b) Severity 2 - every thirty (30) minutes during Support Hours or such other times as may be mutually agreed.

(c) Severity 3 - as agreed with the TfL Group's Nominated Representative (to be named in the Service Model as referred to in paragraph 14 below).

(d) Severity 4 - as agreed with the TfL Group's Nominated Representative.

5.2 Incident Management

The Service Provider shall comply with the following in respect to Incident management:

Measure	Definition of Measure	Achievement Measure	Target Service Levels	Service Credit(s) * applied against Achievement Measure
Severity 1 Incident Respond	For each Severity 1 Incident, the time from a contact arriving at the Service Desk, or from an automated alert, to the time that the Authority (or PSP) is informed that the Incident is being worked on by the appropriate Resolver Group.	Within 15 minutes during the Primary Support Hours	100%	0

Measure	Definition of Measure	Achievement Measure	Target Service Levels	Service Credit(s) * applied against Achievement Measure
Severity 1 Incident Restore	For each Severity 1 Incident, the time from a contact arriving at the Service Desk, or from an automatic alert, to the time that the Incident is Restored, a Workaround is agreed or a Problem Rectification Plan to Restore is agreed.	Within 1 hour during the Primary Support Hours	Within 1 Working Hour for 90% of Incidents and within 2 Working Hours for 98% of Incidents	3
Severity 2 Incident Respond	For each Severity 2 Incident, the time from a contact arriving at the Service Desk, or from an automated alert, to the time that the Authority (or PSP) is informed that the Incident is being worked on by the appropriate Resolver Group.	Within 45 minutes During the Primary Support Hours	100%	0

Measure	Definition of Measure	Achievement Measure	Target Service Levels	Service Credit(s) * applied against Achievement Measure
Severity 2 Incident Restore	For each Severity 2 Incident, the time from a contact arriving at the Service Desk, or from an automatic alert, to the time that the Incident is Restored, a Workaround is agreed or a Problem Rectification Plan is agreed.	Within 2 hours during the Primary Support Hours	Within 2 Working Hours for 90% of Incidents and within 4 Working Hours for 98% of Incidents	2
Severity 3 Incident Respond	For each Severity 3 Incident, the time from a contact arriving at the Service Desk, or from an automated alert, to the time that the Authority (or PSP) is informed that the Incident is being worked on by the appropriate Resolver Group.	Within 3 hours during the Secondary Support Hours	98%	

Measure	Definition of Measure	Achievement Measure	Target Service Levels	Service Credit(s) * applied against Achievement Measure
Severity 3 Incident Restore	For each Severity 3 Incident, the time from a contact arriving at the Service Desk, or from an automatic alert, the time that the Incident is Restored, a Workaround is agreed or a Problem Rectification Plan is agreed.	Within 8 hours during the Secondary Support Hours	Within 8 Working Hours for 90% of Incidents	1
Severity 4 Incident Respond	For each Severity 4 Incident, the time from a contact arriving at the Service Desk, or from an automated alert, to the time that the Authority (or PSP) is informed that the Incident is being worked on by the appropriate Resolver Group.	Reasonable endeavours only during the Secondary Support Hours		

*to determine Persistent Breach

5.3 Problem Management

The Service Provider shall comply with the following in respect to Problem Management:

Measure	Definition of Measure	Achievement Measure	Target Service Level	Service Credit(s)*applied against Achievement Measure
Severity 1 Problem Resolution	The time from a contact arriving at the Service Desk, or from an automatic alert, to the time that the Problem is fully Resolved and an RFC raised for the Implementation, or that the Problem is identified as a Known Error, or that a Problem Rectification Plan is agreed with the Authority, where the Root Cause is known, (or the TfL Group's PSP), who shall not unreasonably withhold such agreement. Where the Root Cause is not known the Provider must perform Root Cause Analysis in keeping with the assigned Severity and the Authority will expect update(s) at a frequency to be agreed between the parties.	Within 1 Business Day	100%	3

Measure	Definition of Measure	Achievement Measure	Target Service Level	Service Credit(s)*applied against Achievement Measure
Severity 2 Problem Resolution	The time from a contact arriving at the Service Desk, or from an automatic alert, to the time that the Problem is fully Resolved and an RFC raised for the Implementation, or that the Problem is identified as a Known Error, or that a Problem Rectification Plan is agreed with the Authority, where the Root Cause is known, (or the TfL Group's PSP), who shall not unreasonably withhold such agreement. Where the Root Cause is not known the Provider must perform Root Cause Analysis in keeping with the assigned Severity and the Authority will expect update(s) at a frequency to be agreed between the parties.	Within 5 Business Days	100%	2

Measure	Definition of Measure	Achievement Measure	Target Service Level	Service Credit(s)*applied against Achievement Measure
Severity 3 Problem Resolution	The time from a contact arriving at the Service Desk, or from an automatic alert, to the time that the Problem is fully Resolved and an RFC raised for the Implementation, or that the Problem is identified as a Known Error, or that a Problem Rectification Plan is agreed with the Authority, where the Root Cause is known, (or the TfL Group's PSP), who shall not unreasonably withhold such agreement. Where the Root Cause is not known the Provider must perform Root Cause Analysis in keeping with the assigned Severity and the Authority will expect update(s) at a frequency to be agreed between the parties.	Within 10 Business Days	98%	1

*To determine Persistent Breach

6.   Incident and Problem Management

6.1   The parties will work together to define and agree a service model, to be updated from time to time by the Parties, which encapsulates the ITIL best practice for end-to-end service delivery and support which will include Incident and Problem management.

7.   Escalation Management

7.1   The parties will work together to define and agree a service model, to be updated from time to time by the Parties, which encapsulates the ITIL Best Practice for end-to-end Service Delivery and Support which will include Escalation Management. Such model shall take into consideration the Dispute Resolution Procedure including **clause 38.2**.

8.   Configuration Management Database (“CMDB”)

8.1   The Service Provider shall ensure that where Releases are delivered to the Authority, they will deliver such information as is required to update the TfL Group's CMDB reflecting changes made. This covers but is not restricted to Software version numbers, documentation, and licensing.

8.2   The Service Provider shall ensure that where changes to the Software are made as a result of Fault or Software Error correction, they will deliver such information as is required to update the TfL Group's CMDB reflecting changes made.

9.   Reporting

9.1   The Service Provider's Nominated Representative shall provide the TfL Group's Nominated Representative with a Periodic Service Report within five (5) days of the end of each Measurement Period indicating:

(a)   number of requests for Support, by Severity;

(b)   number of requests cleared;

(c)   number and status of outstanding requests;

(d)   average time to Respond by Severity;

(e)   average time to Resolve by Severity;

(f)   performance against Service Levels as specified in paragraphs 5.2, 5.3, and 15.4 of this **Annex B** of **Schedule 2**;

(g)   Service Credit report;

(h)   such further matters as the Authority may reasonably require.

9.2   The Authority may request that the Service Provider supply information relating to Major Incidents to the TfL Group's Primary Service Provider. This information shall include diagnostic procedures and resolution details. Such information to be provided for inclusion in Major Incident Reports to be produced by the TfL Group's Primary Service Provider and shall be made available to the Service Provider upon reasonable request.

9.3   The Service Provider will arrange a service review meeting to be held within the ten working days following the end of each Measurement Period (**"Service Review Meeting"**) with the Authority at a Site unless mutually agreed otherwise. The agenda for this meeting will include: performance monitoring; summary of activity (lessons learnt, recommendations for Software or service change); Service Credits (as set out in paragraph 19 below) and any other related topics as notified by either party. The Authority shall take minutes of such meetings and distribute them to the Service Provider.

10.   Change Management

10.1   The parties will work together to define and agree a service model which encapsulates the ITIL Best Practice for end-to-end service delivery and support which will include change management.

11. Versions and Releases

11.1   The Service Provider will notify the Authority of each new Version or Release of the Software, which from time to time is made available by the Service Provider to users generally.

11.2 The provision of each new Version or Release during the Term is included in the Charges.

11.3 Under this Agreement, the Authority is entitled to migrate to new Versions of the Software released by the Service Provider during the Term.

11.4 Whenever a new Version of the Software is released, the Service Provider will notify the Authority and will inform the Authority of the implications that the new Version will have on the Software and provide Release Notes. The Service Provider will ensure that new Versions of the Software will maintain the functionality of previous Versions unless expressly agreed with the Authority in writing. The Service Provider will ensure that the new Version of the Software will be able to read the files of the previous Versions.

11.5 With the acceptance of the migration to a new Version, the Authority is entitled to specify when the new Version of the Software will be introduced which must be within a period of six (6) months after its acceptance.

11.6 If required by the Service Provider the Authority will, after the TfL Group's installation and acceptance of a new Version or Release, either return the previous Version or Release and all copies of the whole or any part of it or destroy it and certify in writing to the Service Provider that this has been done.

12. Scheduled maintenance/Ad-hoc downtimes

12.1 All downtime must be scheduled and approved under the Authority Change Management process (which will be notified to the Service Provider within the service model referred to in paragraph 14.1) and shall be authorised by the Authority unless it is part of a major incident recovery plan.

13. Nominated Representatives

13.1 For the purposes of receipt of the Maintenance Services, the TfL Group's Nominated Representative shall be the Contract Manager as stated in **Schedule 1**.

13.2 For the purposes of provision of the Maintenance Services, the Service

Provider's Nominated Representative is: **Stephen McGrath.** The Service Provider undertakes to keep the Authority informed of any changes to their Nominated Representative.

14. Service Model

14.1 It is expressly the intention of the parties to work together to define and agree a service model which encapsulates the ITIL Best Practice for end-to-end Service Delivery and Support.

14.2 The Authority have outsourced responsibility for certain of the TfL Group's IT environment to its Primary Service Provider. The scope of services provided under this arrangement includes: service desk; desktop support; infrastructure (server; LAN/WAN, messaging); and applications. The Authority expects that initial contact will be made to the Service Provider via this Primary Service Provider. Management of problems, incidents, change/release will be via this Primary Service Provider.

14.3 The Authority wishes to ensure that the TfL Group Users do not suffer any adverse impact on Services provided to them under this Agreement as a result of the interface between the Service Provider and the Primary Service Provider. Accordingly, it is expressly the intention of the Authority that the Service Provider enters into an Operational Level Agreement (**"OLA"**) with the Primary Service Provider to ensure that end-to-end Service Levels are achieved in respect to Problem and Incident resolution. The Service Provider agrees with the Authority that the Service Provider shall comply with its obligations under the Operational Level Agreement.

15. Availability, Capacity and Service Assurance Activities

15.1 The Software will be available during the Support Hours subject to the remaining provisions of this paragraph 15 and the Maintenance Services will be provided during the Support Hours. The Service Provider warrants that it has the capability to provide the Maintenance Services during the Support Hours subject to any request by the Authority for such availability being dealt with under the change control provisions of this Agreement.

15.3 **Calculation of Availability and Availability Levels**

Availability shall be calculated as a percentage of the Primary Support Hours minus any agreed downtime in a Measurement Period. Failure to achieve the Availability Target of 99.88% in a Measurement Period shall result in 3 Service Credits.

15.4 **Other Service Levels**

15.4.1 The table below sets out certain Service Levels which the Service Provider shall meet or exceed in providing the Services.

15.4.2 Each Service Level is measured over the Measurement Period, except where stated otherwise.

Service Levels:

Ref	Service Level Name	Service Level definition	Measure(s)	Metric Service Level
1	Security activities.	The Service Provider will carry out security and system administration activities forming part of the Services in accordance with the Measures listed in the next column (**"Measures")**. Without prejudice to any other remedy of the Authority or obligation of the Service Provider for breach of Service Levels, if the Service Provider	(a) No security incidents occurring owing to inappropriate TfL Group User permissions. (b) Each security patch delivered as required unless the Authority directs otherwise. (c) No administration passwords in use for longer than 3 months. (d) No inactive or unauthorised accounts.	At least 3 of the 4 Measures must be met
		fails to comply with this Service Level the Service Provider shall before the start of the next calendar month		

		produce a documented service improvement plan for the impacted Service Levels and, once agreed by the Authority in writing, promptly implement such plan		
2	Customer Satisfaction Scorecard score.	The Authority may from time to time provide the TfL Group Users with Customer Satisfaction Scorecards (the form of which shall be agreed with the Service Provider prior to first use).	All Customer Satisfaction Scorecards will show an TfL Group User rating of the Services as 'satisfactory' or higher.	80% of TfL Group Users ratings score as 'satisfied' or higher in TfL Group User surveys.
		The Service Provider will achieve a level of response in accordance with the Measure for each Customer Satisfaction Scorecard survey carried out.		

	Call abandonment rate.	The Service Provider shall seek to minimise the number of calls for support from the Authority which are abandoned by TfL Group.	100% minus X, where X is the percentage of all calls received by the Service Desk that are abandoned by the caller after a 15 second period has elapsed from the point that the call is received or after any agreed initial announcement/menu has ended.	No more than 4% of Calls are abandoned.
3		Users/the applicable TfL Group representative or agents before being answered, in accordance with the Measure.		
4	Major Incident Report	The Service Provider shall ensure that the period from the Restore time in respect of each Severity Level 1 or 2 Incident to the delivery of the Major Incident Report to the agreed Authority recipient will be in accordance with the Measure.	All Major Incident Reports for Severity Level 1 and 2 Incidents will be delivered within 3 Business Days of the Incident Restore time.	90%

5	Response to RFCs, including project scoping requests, non standard products and RFIs (for legislative requests).	The Service Provider shall ensure that the time from receipt of the RFC to implementing the requested action or providing a response to the request indicating timescales for implementation agreed with the applicable TfL Group representative or agents are in accordance with the Measure.	All requests will be implemented within 3 Business Days or, if not achievable within 3 Business Days the Service Provider will provide a response within 3 Business Days from time of Service Request indicating and agreeing the time to implement with the applicable TfL Group representative or agent.		80%
6	Capacity Management	The Service Provider shall ensure that agreed capacity levels are maintained in accordance with the Measure.	No capacity levels will be allowed to fall below the agreed threshold levels in the Specification, if any, except by prior notification to and agreement with the Authority.		100%
7	Agreed Server "housekeeping activities"	The Service Provider will carry out all activities specified in the "Measure" column in accordance with the Measure.	Configuration Items updated in the CMDB by the Service Provider shall be accurately updated. [Other activities to be entered here]		100%

| | | Without prejudice to any other remedy of the Authority for breach of Service Levels, if the Service Provider fails to comply with this Service Level the Service Provider shall within a timescale agreed with the Authority produce a documented service improvement plan for the impacted Service Levels and, once agreed by the Authority in writing, promptly implement such plan. | [This Service Level is based on the percentage of the above Measures that have been met in all regards in the relevant Calendar Month. **"In all regards"** for this purpose means that (i) the activity specified for a Measure above has been completed; and (ii) any obligations contained in any service improvement plan due to be performed in the relevant month in respect of that Measure have been successfully completed.] | |

16.   Place for Provision of Maintenance Services

16.1   As a general rule, all Maintenance Services will be rendered at the Service Provider's premises.

16.2   If the parties so agree or when it is absolutely necessary, Maintenance Services shall be rendered on site at the TfL Group's premises.

16.3   Any travel needed to provide services at the TfL Group's premises will be made as soon as possible, depending on the urgency of the Maintenance Services required and of the availability of the Service Provider, but not later than eight (8) Business Days after the date when the parties have agreed on the need for travel.

16.4   The Service Provider warrants that its members of staff and/or third parties it employs shall not perform any activity at the TfL Group's premises without supervision by and/or explicitly prior to approval from persons authorised by the Authority.

16.5   The Service Provider shall then perform its activities taking into account the instructions given by the Authority.

17.   Introduction of Small Functional Adjustments to the Software

17.1   New functionalities in the Software must be requested in writing by the Authority, describing the adjustment to be introduced in the Software.

17.2   Within a maximum period of ten (10) Business Days after the date of a request for a variation to the Software by the Authority, the Service Provider will evaluate the feasibility of the required change and provide a quotation to implement the required changes including its estimate of the Man Hours and time required to implement such adjustment. Such changes shall be subject to Change Control Provisions in **Schedule 7** and initiation of such changes will commence within twenty (20) Business Days of the execution of a Change Control Note, unless agreed otherwise. The Service Provider shall comply with reasonable requests by the Authority to perform any work in accordance with the TfL Group's Change and Release Management process as set out in the

service model to be defined and agreed following execution of this Agreement.

17.3 The Service Provider will not implement the adjustment before the acceptance of the estimate by the Authority and execution of a Change Control Note.

17.4 Notwithstanding the estimate provided by the Service Provider, the actual time spent by the Service Provider in carrying out the evaluation and providing the quotation together with time spent implementing the required adjustments will be charged to the Authority at the Extra Work/Additional Support rate set out in **Schedule 3**. The Service Provider will not be entitled to exceed the quotation without the prior agreement of the Authority.

17.5 The Authority will test the functional adjustment in accordance with **Schedule 6** or such other arrangements as the parties may agree.

17.6 The Authority will review the deliverables against the acceptance criteria in **Schedule 6**. The Authority reserves the right to accept and/or reject such deliverables. The Authority will advise why such deliverables are rejected.

17.7 For the purposes of Service Credit measurement, a Service Credit of two (2) per request for change will be applied for non-compliance with the time periods specified in paragraph 17.2.

17.8 The maximum number of Service Credits for which the Service Provider will be liable under paragraph 17.7 will be limited to ten (10) Service Credits in any one Quarter, no matter how many requests for change the Authority submits.

18. Major Adjustments and Exceptional Activities

18.1 The rendering of services concerning Major Adjustments and other activities which do not fall under the scope of this Schedule and shall be subject to Change Control Provisions in **Schedule 7** or by way of Additional Services, as may be agreed between the parties in writing.

19. Service Credits

19.1 Should the Service Provider fail to meet any of the Service Levels set out in this Schedule the Authority will receive Service Credits in accordance with

paragraph 20. Service Credits will not become due if failure to meet a Service Level is due to:

- faults caused by the actions or omissions of the TfL Group or third parties not under the contractual control of the Service Provider;

- faults in equipment and systems not supplied by the Service Provider or its agents;

- viruses other than those introduced by the Service Provider or its agents;

- malicious activity of the TfL Group or third parties not under the contractual control of the Service Provider;

- the Authority failing to permit the Service Provider adequate access to Site and/or the Software; or

- the Service Provider being unable to remedy a notified Fault due to the acts or omissions of the TfL Group or third parties not under the control of the Service Provider.

19.2   This **Annex B** of **Schedule 2** sets out the Service Levels which the Service Provider shall meet in each Measurement Period and the applicable Service Credits which the Service Provider shall pay to the Authority should it fail to meet various of the Service Levels (including the various categories within such Service Levels) in the applicable Measurement Period. The Service Provider will provide to the Authority within five (5) days of the end of the relevant Measurement Period a breakdown of the Service Levels missed within that period, if any, and the details as to the extent they were missed (expressed in minutes or percentages as applicable) together with the applicable Service Credits due. The resulting Service Credit figure will be used to calculate the Service Credits.

19.3   In the event of multiple Incidents resulting from a common cause, or in the event of one Incident causing the failure of the Service Provider to meet more than one Service Level, then only the Service Credit most advantageous to the

Authority shall apply.

19.4 For the avoidance of doubt, the elements of Service that attract Service Credits are as defined in paragraphs 5.2, 5.3, 15.3 and 17.7 above or as otherwise expressly set out in this Agreement.

19.5 The Service Credits shall be without prejudice to any other right or remedy the Authority may have including without prejudice to the generality of the foregoing the right to receive damages.

20. Service Credit Amounts

20.1 The Service Provider shall reduce the next Charges due to it from the Authority by the amount of Service Credits accrued in the previous Quarter. Where no further charges are due, the Service Provider shall issue the Authority a credit note to the Authority for the Service Credit amount within thirty (30) days of the end of the relevant Quarter.

20.2 The sum of Service Credits payable to the Authority in each Contract Year shall not exceed be 20% of the Total Annual Charges payable by the Authority to the Service Provider. Service Credits may still be accumulated.

SEVERITY LEVEL	SERVICE CREDITS (To be recorded for the purposes of determining Persistent Breach)	SERVICE CREDIT AMOUNT
Severity Level 1 Restore	3	An amount equal to **5%** of the Charges payable to the Authority during the relevant Contract Year.
Severity Level 2 Restore	2	An amount equal to **3%** of the Charges payable to the Authority during the

		relevant Contract Year
Severity Level 3 Restore	1	An amount equal to **1.0%** of the Charges payable to the Authority during the relevant Contract Year.

21. **Persistent breach of service levels**

21.1 Without prejudice to the TfL Group's other rights and remedies it may have (including any rights to terminate the Authority shall be entitled to) the Authority may terminate provision of the Maintenance Services forthwith by giving written notice to the Service Provider in the following circumstances:

	PERSISTENT BREACH
	a) Failure to meet a Service Level for 3 consecutive Measurement Periods; or b) Failure to meet a Service Level for any 3 Measurement Periods in any Contract Year; or c) Accumulation of 15 or more Service Credits for any Service Level in 3 consecutive Measurement Periods; or d) Accumulation of 15 or more Service Credits for any Service Levels in aggregate in 5 Measurement Periods in any Contract Year Each breach, under a) and b) of this clause, shall require a service rectification plan to be developed and , subject to the agreement of the Authority, implemented by the Service Provider within 5 Business Days to resolve the Service Level breach. The successful implementation of the service rectification plan shall end

	subject to clause 21.2, the Authority's right to terminate under this agreement, In the event of a breach pursuant to c) and d) of this clause, the Authority's right to terminate will remain in force for ninety (90) days following the 5th (or subsequent) Period in which the volume of Service Credit accumulation exceeds the stated level.

21.2   Failure by the Authority to exercise a right to terminate shall not prevent the Authority from exercising its right to terminate under this **Annex B** of **Schedule 2**:

21.2.1 at a later date in relation to a separate or subsequent breach (whether or not committed in similar circumstances); or

21.2.2 at any time pending the satisfactory completion of an agreed service rectification plan relating to the persistent breach in question.

21.3   Following any such termination, the Service Provider shall promptly pay to the Authority a refund of any Charges for the Maintenance Services paid in advance in respect of the period following termination.

ANNEX C

ADDITIONAL SERVICES

2.   **SERVICE PROVIDER'S OBLIGATIONS**

2.1   The Service Provider shall provide such Additional Services as specified in **Schedule 1** upon payment of the Additional Services Charge specified in or calculated in accordance with **Schedule 1**.

2.2   The Additional Services may take the form of all or any of the following:

   2.2.1   the provision of a set number of man days of consultancy (whether for the preparation of further or bespoke software, a software specification or otherwise) as specified in **Schedule 1;**

   2.2.2   the supply of further or bespoke software, a software specification, or such other items as specified in **Schedule 1;**

   2.2.3   the provision of training and consultancy services as specified in **Schedule 1**.

2.3   The provision of the Additional Services by or on behalf of the Service Provider for the Authority shall be subject to the terms of this Agreement.

ADDITIONAL SERVICE CHARGES

   The Additional Services Charges shall be levied by the Service Provider for the Additional Services provided by the Service Provider as set out in **Schedule 3**.

SCHEDULE

3 Charges

F9857H98

SCHEDULE 4

Statement of Requirements

Transport for London

SCHEDULE 4

Multi Modal Integrated Command and Control System (MICCS)

Statement of Requirements

Transport for London

Table of Contents

Transport for London

Transport for London

Document Control

0.1. References

Ref	Title	Location
1	Data Retention Schedule for Health and Safety	Included as Appendix
2	TfL Information Security Classification Standard	Included as Appendix
3	TfL IM Security Policy: Patch Management (IM-S-PO-019)	Included as Appendix
4	TfL IM Security Policy: Software Development	Included as Appendix
5	Licence Requirements for TfL Software Procurement	Included as Appendix
6	Information Security Control Framework – supplier version	Included as Appendix
7	TfL Information Security Policy	Included as appendix
8	TfL Change Management Process	Included as Appendix
9	TfL Release Management Process	Included as Appendix
10	LU Rule Book 2 Managing incidents	Included as Appendix
11	SMS integration using SOAP/ XML protocol via PageOne API	http://www.pageone.co.uk/developers/api-library
12	Information Security Control Framework	Included as Appendix
13	Example reports a. Area delays daily (CentreComm) b. NDM Daily Report (CentreComm) c. Ticket Holder Requests (CentreComm) d. Ambulance report – record of all ambulance requests from 02.00 to 02.00. Distributed daily. (LUCC) e. Security report – record of all security incidents from 07.00 to 07.00. Distributed daily. (LUCC) f. SPAD report – record of all SPADs from 02.00 to 02.00. Distributed daily. (LUCC) g. Cat One response spreadsheet – tracking performance of Cat One incidents. (LUCC)	Included in Appendix
14	Example of Area, duties loaded	Included in Appendix

Transport for London

Glossary

Type: T = term, E = Entity, TfL = TfL term

Term	Type	Description
Action List	T E	The list of activities that should be completed against a specific incident type. Example: Person Under Train (PUT) incident type will require the following steps: • Emergency services and LU staff called and en route – BTP, LAS, LFB, NIRM, ERU, duty managers • Treatment/removal of casualty • Removal of casualty from trackside • Cleanup Attributes Include but are not limited to; • Action description, e.g. o NIRT deployed o NIRT on site o Cat 1 implemented o Called Customer Service Centre to notify incident. o End of Formal Incident Management declared for a Cat 1 o Advised of Service resumption & Status; Good Service, Minor Delays, Severe Delays • Assigned to, Completion status
APD JNP Incident Engineer	TfL	Part of the LU Control Centre, have their own IT infrastructure, plus read only on current NIMROD, previously Tubelines Incident Manager.
Bulletin Board	T	External facing communication, possibly a website / portal, where detail of diversions, incident, ticket requests can be published to. Access is password controlled. The data is not TfL_Restricted, but may support operational decisions taken in garages (for example) or affect the shift of bus drivers.
Candidate Incident	T	An incident that is offered as a potential for: • Duplicate incident; multiple calls received about the same incident, close down all but one incident • Linked incident: associated (linked) incidents, both are managed independently • Previous incident: previous occurrence of a similar incident, want to reference to help answer the questions "what did we do last time this happened? Do we have a component that keeps failing? "

Transport for London

Term	Type	Description
Category One Incidents (LU only)	T	Require formal incident management, as outlined in the LU Rule Book 2. A Category One must be declared if there is the potential (as of Issue 4) for: • Trains to be stalled for more than 30 minutes or • Full or partial line suspensions, or • Serious infrastructure damage, or • Serious injury or loss, or • More than one line, multiple locations to be affected. Or for: • A radio system failure • Major power failure • Major flooding incident • Confirmed terrorist attack • Major fire • An evacuation of the Underground • A person under a train.
Communication Recipient	T E	A person that receives a communication from a control centre: • Via access to the Bulletin Board (CentreComm only) • Via an SMS or email on a status or incident, or • Has no system access – other than self registration for access to the Bulletin Board. Attributes include but are not limited to: • Name • Organisation (TfL, bus operator, maintenance contractor etc) • Recipient email address • Recipient mobile telephone number • Access to the Bulletin Board
Contingency Plan	E	A planned response to an incident, prepared in advance, to be invoked as required. Include but are not limited to: • Textual description of plan • Action list to be mapped to incident / event when invoked • Pictures to be referenced when a plan is being implemented GIS map to be referenced when a plan is being implemented
Critical National Infrastructure	T	The Government defines CNI as: "Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life"

Transport for London

Term	Type	Description
CPNI	TfL	Centre for the Protection of National Infrastructure, protects national security by providing protective security advice. (http://www.cpni.gov.uk/about/cni/
Dashboard	T	A user interface that somewhat resembling an automobile's dashboard organises and presents information in a way that is easy to read. The solution will require multiple dashboards to be definable.
Desk Log	E T	Any activity or information that is worth recording, any information that an Operator wishes to formally record in the solution. A Desk Log entry is created when an Incident is not appropriate to use. For attributes, see Desk Log data.
Diversion	T	A temporary change to a Bus Route. (CentreComm only)
Diversion Reference Number	T	This is required by TfL Performance and acts as 'authorisation' for the diversion. I.e., without this diversion reference number, TfL Performance will not accept the diversion as legitimate, and the Bus Operator will not get paid for any lost mileage.
Duty	T	A predefined work pattern, e.g. a repair van or a BSC (Bus station controller) shift. Resources are booked onto a Duty and shift. Attributes include but are not limited to; • Duty name (CE04) • Duty description (Camden and Islington) Middle duty Aldgate bus station • Early turn (times) e.g. 0600-1342 • Late turn (times) e.g. 1330 - 2142 • Default mobile number • Polling frequency, in minutes: e.g. at least once every 10 minutes • Logged in status • Availability status.

Transport for London

Term	Type	Description
EIRF System	TfL	The Electronic Incident Reporting Form known as EIRF is a web based application, which allows over 3500 registered Train and Station staff users to log incidents, which occur during the daily operation of the railway. EIRF is implemented using the Metastorm BPM product suite, a specialist software development tool for automating business processes and workflow systems. It processes to be designed and specified in a graphical environment, the Process Designer. From these process 'maps', Metastorm automatically generates database tables, business rules and user interface customisation.
		This information is then used to measure the performance of the railway. Data feed are:
		CUPID – New data from EIRF is pulled into CUPID at 06.45, 09.45 and 12.45 each day.
		LUSEA – Data is pulled from EIRF on an hourly basis.
		Heartbeat – A Daily Summary Report is produced by EIRF as a PDF file and this can then be accessed using Heartbeat reporting
Emergency Alert	T E	A one way message sent out simultaneously in an emergency
		Attributes include but are not limited to;
		• Recipient group,
		• Message text,
		Response status / recipient.
ERU	TfL	Emergency Response Units in LU network incidents
Event	T E	An Event is an activity that the users are aware of. It is mainly a planned activity that the user knows is going to happen on a given date and time (e.g. London Marathon, Road works, London Underground terrorist attack simulation).
		Attributes include but are not limited to;
		• Start date and time of the event,
		• End date and time of the event,
		• Event Type Drop down,
		• Event description, Free text,
		• Event location, Drop down or a free text location),
		Control Area/Line, Drop down.
		Created by LUCC users. (Note, difference with Notice of Event)
FOIA	T	The Freedom of Information Act gives the public the right to access information held by TfL. Note: there is no automatic link between a security classification and an exemption under the Freedom of Information Act (FOIA).
I-LCH	TfL	Indicative Lost Customer Hours (reported on LUCC Daily Performance Review)

Transport for London

Term	Type	Description
IMPACT	TfL	IMPACT is the spatial repository used by EOS (Enforcement and On street Safety, previously) Community Safety and Enforcement Policing (CSEP) to visualise, analyse and report transport related crime and congestion incidents throughout London's Metropolitan and surrounding areas.
IM	TfL	(TfL) Information Management.
IMPULSE	TfL	The Incident Management Planning User System (IMPULSE) defines review and response plans for incident management and recovery. These are supported by Action Lists.
Incident	T E	Any failure, defect or malfunction on the service, or an unplanned occurrence on a Bus or Network, or information circulated to CentreComm. For attributes see Incident data.
Incident Type	T	Describes the incident, e.g. Person under train, power loss. The incident type will indicate the type of actions required from the control centre in response. Previously referred to as Cause Code within CentreComm
Incident Activity	T	Any activity undertaken in response to an Incident
Incident Activity Log	T	A record of each activity performed or notified during an incident. There could be many activities created as an incident progresses. The Incident Activity creates an audit trail. Example: who did what, what was done against an incident.
Incident Activity Template	T	A template or predefined form that is completed when requesting a service, e.g. ambulance, police, ERU, LFB, replacement bus service, or a commonly performed Incident Activity. (Centrecomm have indicated they would not use the template / Proforma function initially. Their response plans tend to be less complex.)
Incident Queue	T	A list of incidents. Can be, based on status or on the user role; including but not limited to; • NRT list, CentreComm incident assigned to the NRT for follow up, • NOM list, LUCC incident assigned to the NOM for review and closure.
Incident Reference Number	T	Reference number quoted by the Operator when passing details of an Incident to an emergency service.
InfoLink	TfL	Nexus Alpha tool providing access to TOC (train operating company) service status. Access to this helps LUCC identify potential impacts on LU services, e.g. taking tickets may be required.
Live Information Desk (LID)	TfL	Live Information Desk (LID) is a twitter team, based in CentreComm who send out public information on the status of the bus network. They will record their activity on their own Desk Log.
Line Control Centre	TfL	This is a control centre where the day to day operation of an LU line is controlled and monitored.
Line of Route	T	The normal route taken by a Bus.

Transport for London

Term	Type	Description
Level of Visibility	T	An incident ant any content associated with it can be assigned a level of visibility, i.e. which Role Type(s) the incident, or the existence of the incident is visible to.
Location Code	T	Location codes are shared in the telephone calls to the London Fire Brigade and the London Ambulance Service. Currently no location codes shared with the BTP. Also referred to (by LUCC and LFB/LAS) as "HLUL codes"
Location Directory	T	The list of locations in the system, including stations, LUCC and Line Control Centre addresses and all other addresses that are relevant. Holds location codes shared with the London Fire Brigade and the London Ambulance Service.
LU	TfL	London Underground
LUCC	TfL	London Underground Control Centre, previously known as NOC Network Operations Centre
LU line	TfL	Including but not limited to: Jubilee, Northern, Piccadilly, Bakerloo, Waterloo & City, Central, Victoria, Circle, Hammersmith & City, District, Metropolitan Lines
Map Extents	T	The option of the map shown with full mapping detail. TfL do not require the full UK mapping detail, and do not wish to be available to search on all streets on the UK. The Map Extent will define the area where full mapping detail is required.
Masternaut	TfL	A Tubelines application that tracks the location of the ERUs
NCI	TfL	Network Customer Information
Network Operations and Control	TfL	Dept for both LU CC and Contingency Planning, responsible for contingency planning and Weather readiness plans.
NIMROD	TfL	Network Incident Monitoring Real-time Operation Display. It records incidents that affect the operation of the railway which allows the LUCC users to create, view, update and search for incidents
NOC	TfL	Network Operations Centre, now known as the LU Control Centre (LUCC)
Notice of Event (NOE)	T	A planned response for buses to a planned Event, created by Event Planning Team and issued by Area Managers for Surface, mostly pre-planned roadworks, 100/200 a week. Geo-located to the nearest bus stop. If available from the CDR, the functionality to load from SharePoint can be removed)

Transport for London

Term	Type	Description
Notify to Duty Manager	T	Where an incident is flagged for the attention of the Network Duty Manager (No connection to a notifiable incident from a RIDDOR, Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995 perspective) (Previously "Notifiable" in CentreComm)
Operator	T	Staff taking a call in the Control Centre; logging incidents, co-ordinating a response, notifies 3rd parties and deploys resources as necessary.
OTP	TfL	Other Transport Providers
PageOne	T	PageOne is a web accessed, online text system which enables LUCC and CentreComm to send service information messages, staff information messages and other transport provider messages to email addresses and mobile phones.
Postal Area Code	T	For London this will take the form of Postcode Area and Name – examples: • E8 Hackney • N7 – Holloway Refer to: http://en.wikipedia.org/wiki/London_postal_district For Greater London, this will take form of Postal Area Name – examples: • CR – Croydon • BR – Bromley
Recipient List	T E	Group of Communication Recipients for a specific type of communication; e.g. All SOO (LUCC) or bus operators. Attributes includes but are not limited to: • Recipient list name (e.g. "All SOOs") • List description • Communication Receipts in the list – note these contact details will not be used initially for the SMS/Email service. • Relevant tags, e.g. "Victoria line"
Region	E	A London area e.g. "Central", "South", "North" Duties and Resources are managed

Transport for London

Term	Type	Description
Resource	T	Currently, only CentreComm deploy On Road Bus Operations resources to assist with the management of Incidents at the scene. The following Types of Resource may be deployed including: • - Network Traffic Controllers (NTCs) - the 'eyes and ears' on the road of the control room. They provide vital, on site information and support for any incidents or planned events, 24 hours a day cross the whole of London. • - Tow Truck – a vehicle recovery service for Buses that become inoperable. • - Cleaners –can be deployed to deal with any on Bus incident that requires cleaning services. Attributes include but are not limited to: • Resource type • Resource name • Badge No Note – a Duty, not a Resource logs in and out, and is available or not available
Role Type	T	Predefined roles within the solution with authorisation to perform a set of tasks. A user may be assigned one or several Role Types
RPO	T	Recovery Point Objective, RPO, is the maximum tolerable period in which data might be lost from an IT service due to a major incident
RTO	T	Recovery Time Objective, RTO is the amount of time the business can be without the service, without incurring significant risks or significant losses
Safety Integrity Level (SIL)	T	Is a measurement of performance required for a Safety Instrumented Function or System (SIS). A SIS consists of an engineered set of hardware and software controls which are especially used on critical process systems. A critical process system can be identified as one which, once running and an operational problem occurs, the system may need to be put into a "Safe State" to avoid adverse Safety, Health and Environmental(SH&E) consequences. For example SIL rating would be relevant for software or equipment that could introduce a hazard.
Shift	E	Shift , or turns, as assigned to a Duty, data includes is not limited to; • Name e.g Early turn, Middle turn, Late turn, Day turn • Start time End time
SIMLINK	TfL	SIMLINK is a point to point instant messaging system, installed between LU Control Centre and the Line Control centres. It uses a dedicated terminal and connectivity. It was installed 20 years ago in the aftermath of the Kings Cross disaster.

Transport for London

Term	Type	Description
SMS/ Email Message	T E	A text or email sent out to a defined group of recipients. One way communication. Attributes include but are not limited to; • Message type • Recipient group • Message text
SOO	TfL	Senior Operating Officer in the LUCC
Station Directory	T	See Location Directory
Sysfail	TfL	Application used to generate codes that the bus garages need in order to unlock "time locked" ticket machine modules.
Ticket Request	T	A request raised by a Train Operating company for TfL Buses to accept valid tickets on alternate Bus Routes following service disruption.
Ticket Request Pre-Pay Number	T	Identifies a valid Ticket Request to the operator
Traffic Circular	TfL	The weekly Traffic Circular contains diverse information such as, infrastructure changes, train service changes, events affecting LU, notification of restrictions to LU operations and operational communications.

Weather Readiness Plan	T
	
	E
		"54321" is a Winter/Weather Readiness Plan, which defines the steps and tracks the status of stations and lines for weather readiness. The status of each line for stations, trains, service control and maintenance and summary information is currently held on a series of spread sheets on SharePoint
		
		Include but are not limited to:
		• Action list
		• Dept
		• Line
		    o stations
		    o trains
		    o service control
		    o maintenance
		• Day
		• Recipient list

XIS	TfL	Extensible Integration Service (XiS) is a TfL software infrastructure service underpinning a set of business and technical services that allow applications to share information, integrate business processes, and maximise investment in integration components.

Transport for London

1. Introduction

Purpose Of This Document

The purpose of this document is to set out the high level requirements of the Authority for the Software and Service which shall be superseded by an agreed full Specification. In the event of any conflict between this Statement of Requirements and any other schedules or annexes, the other schedules or annexes shall take precedence EXCEPT that this Schedule 4 shall take precedence in the event of a conflict with Schedules 12, 13 and 14.

2. Business Context

2.1. TfL London Underground Control Centre

TfL London Underground Control Centre (LUCC) maintains an overview of the status of the London Underground network and takes immediate action where required to mitigate the effects of any incident.

During incidents escalated to the LUCC, LUCC supports the Line Control Centres by summoning and liaising with the emergency services, arranging alternative travel including emergency bus services and organising emergency on-site catering, while disseminating real-time service information.

The LUCC ensures that senior managers/directors are kept informed of the progress of serious incidents, deciding when to escalate the level of response to an incident, to other senior manager levels.

Network Incident Monitoring Real-time Operational Display (NIMROD) was the project to implement the LUCC's Incident Management system, the NSPIS (National Strategy for Police Information Systems) C&C (Command and Control) product. This tool enables the LUCC staff to record incidents that affect the operation of the railway by providing a facility to create, view, update and search for incidents.

The LUCC are responsible for sending emergency messages to the Line Control Centres, in the event of a network wide incident.

The LUCC ensures that senior managers/directors are kept informed of the progress of serious incidents, deciding when to escalate the level of response to an incident, to other senior manager levels

A Read-only web browser version of NIMROD provides a view of incidents to London Underground Managers.

2.2. CentreComm

CentreComm, the London Buses Command and Control Centre, is responsible for providing a world class command and control facility for 8000 buses and 2.3 billion passenger journeys per annum. They are responsible for:

- Providing a 24-hour call centre throughout the year (whenever buses are in service) for reporting and managing all incidents including major accidents and other emergencies for bus drivers and other surface transport staff. Approximately 700-800 incidents are logged per day (from a volume of 1,000 incoming calls), with a yearly increase of 5%-15%.

- Handling calls from bus drivers, emergency services, river services, utilities and councils. CentreComm do not take calls from the general public.

2.3. Project Scope

The project will;

Transport for London

- Implement an incident capture and management facility for the Control Centres with the capability to be rolled out to other control centres,

- Enable incident and response plans to be geo-coded, and viewed on a map,

- Implement an emergency notification method to send an alert to Line Control Centres where acknowledgement is required,

- Make incident progress and service status information available to TfL staff in a messaging / broadcast capability,

- Enable Event and Diversions management including the ability to view on a map,

- Enable the Location Directory to be accessed and maintained,

- Enable the Weather Readiness Plan to be maintained and updated where the plan is invoked,

- Enable a Contingency Plan to be maintained and used in an incident or event,

- Have the potential to support incident / event capture and browsing via a mobile device,

- Migrate any historical incident data to a platform suitable for queries.

The following applications will be de-commissioned;

- NIMROD in LUCC,

- SIMlink in LUCC,

- CIRS in CentreComm;

    o Warren Point IMS

    o Warren point OSIS

- Google Blog, currently used to publish service status to bus operators. Note there are other TfL and non-TfL users referencing the current Google Blog, e.g. the Customer Service Assistants on the Route 24 buses.

Transport for London
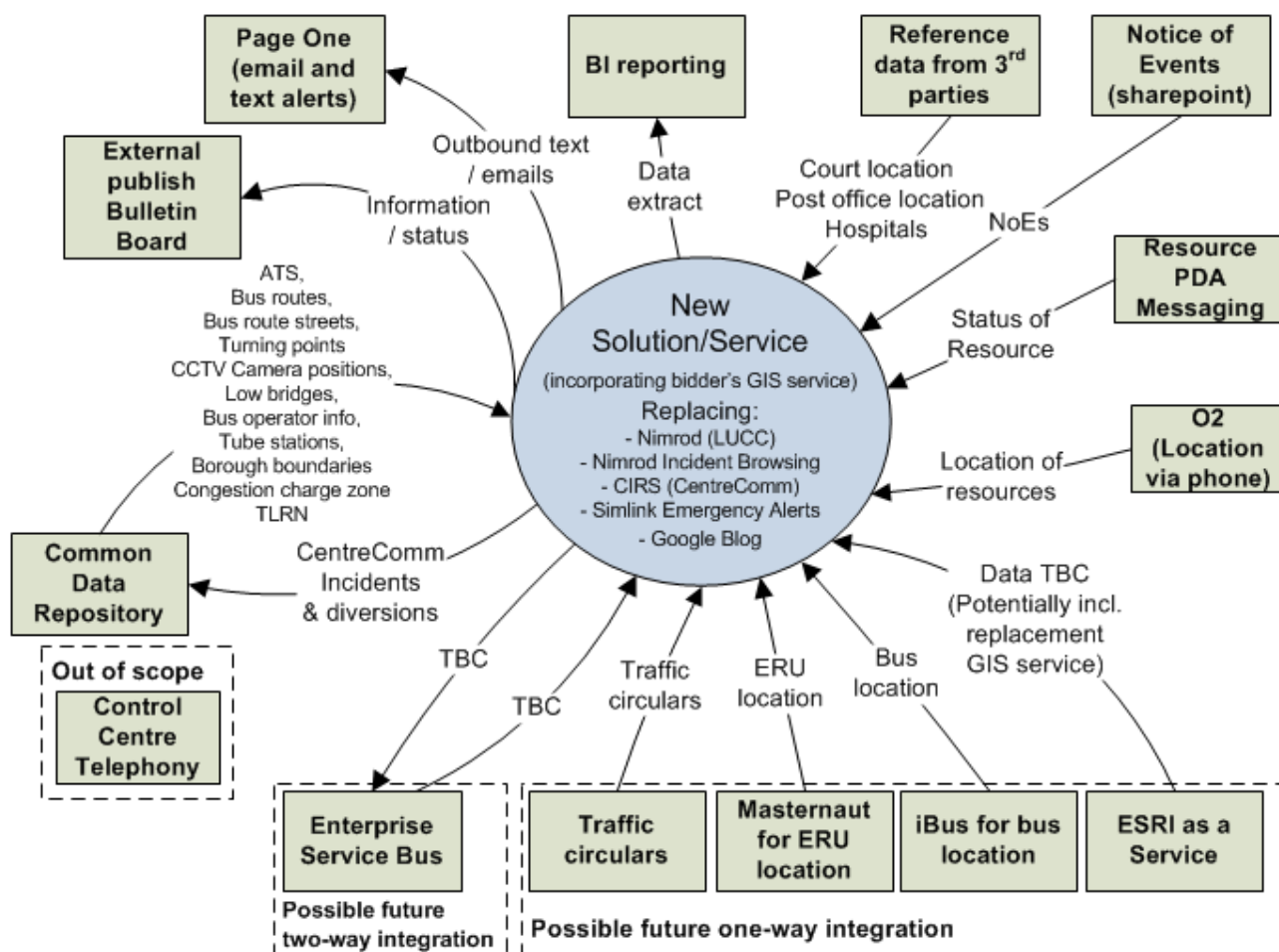
Figure 1, Scope of project for Control Centres systems

The following describe a selection of the interfaces illustrated above:

- TfL Central Data repository, to feed out incident information, and retrieve information on TfL data; bus stops, road networks

- 3rd party data sources public data; e.g. location of courts

- On-street resources' mobile phones to geo-locate resources

- An external bulletin board – may be provided by solution provider

- An SMS service, (currently Page One)

- The on street resources' PDA application to pick up activity

- A TfL SharePoint repository

- TfL business intelligence tool

See Section **Error! Reference source not found.**, **Error! Reference source not found.**, and Section 7, Data required for CentreComm and LUCC, for a further information.

Transport for London

2.4. Possible Future Considerations

The following are described as "Could have" or "Won't have" requirements;

- Integrate with iBus or its equivalent to pull in location and bus details for a bus calling into CentreComm,

- Capability for other control centres and locations to use the solution for incident management,

- Map the position of ERU (Emergency Response Units) on the LU network using their Masternaut location,

- Assignment and management of Incidents to on-street Resources via mobile technology

- Ability to integrate with TfL's Enterprise Service Bus.

2.5. Out Of Scope for the solution

- Integration with any telephony, handling calls to Line Control centres, LU station staff, emergency services, or taxi companies, etc. These are provided via separate resilient services (see below for "Safety and Security Profile" of the services being procured.

- Electronic integration with British Transport Police or any other emergency service, the volume of calls do not justify creating an automated link.

- Any link to an asset system or register.

- Any functionality for Gold Control role function, or who is appointed as Silver Control in a Category One incident

- Maintenance of the recipient lists for SMS/ Email need to be done in the messaging service (a PageOne API is not available for list maintenance)

2.5.1. Out of Scope – LUCC only

- Automated feeds into other incident or reporting systems (except where indicated within this document).

- Replacing the Infolink product currently supplied by Nexus Alpha. This provides TOCs (including TfL) with national rail and network rail status. This allows the LUCC to anticipate and plan for the impact of train delays, e.g. will tickets be required to be taken on the LU network.

- Contingency Plans for the lines and stations.

- Summary of LUCC response and network status, currently via the LUCC managers daily review, no change to this proposed, out of scope for this project,

- Trend analysis and summary reporting, currently done via the Insight's team access to the Line Control Centre's version of incident reports reported via EIRF, no change to this proposed, out of scope for this project.

2.5.2. Out of Scope – CentreComm only

- Cognito PDA field device applications and the messaging gateways which co-ordinate the delivery of data between the devices and TfL (provided by the Mercury solution supplied by O2/Cognito)

Transport for London

- Other applications used by CentreComm e.g. IBUS (includes the Radio System used by the bus drivers).

- External access to the system from 3rd parties (e.g. Bus Operators).

2.6.   Assumptions

1. This project's scope addresses the software systems used to meet the functionality described.

2. The risk profile of the software applications being implemented will not change as a result of the change on delivery method for the functions in scope.

3. No automated interface with the BTP or any other emergency service is required, the volume of calls do not justify creating an automated link.

4. LUCC and CentreComm incident management is not part of the CPNI. The incident tracking system has no requirement for a SIL rating.

5. Manual recording is possible as a back up to record incidents in case of system un-availability, see DP-01 for system restore requirements.

6. Incident data will fall under the remit of the Data Protection Act as personal data could be recorded about individuals involved in an incident, so TfL_RESTRICTED Part 2, see Ref 2.

7. Contingency Plans recorded by LUCC are in the TfL_CONFIDENTIAL category.

8. Information sent out via the broadcast messages and alerts will be TfL_RESTRICTED Part 1.

9. Dual site geographic resilience in a TfL–hosted solution is dependent on the completion of and delivery of the Service Stabilisation Project delivering a second TfL data centre (DCB). UPDATE: TfL would like to clarify that the second data center DC (b) is now in place and the scope does indeed include a second system to be deployed in a second data center.

10. SIMlink replacement functionality needs to deliver resilience to at least the same level as the existing SIMlink function, see below.

11. A Software As A Service SaaS solution provided over the internet is not considered suitable, due to the lack of control over internet access service levels.

12. None of the functions in scope are considered Safety Critical. See section below for discussion on safety profile. Note that the telephony used in the control centres are critical for the management of incidents and are provisioned separately.

13. Access to the back-office applications will be from TfL OneLondon desktop devices (as detailed by the End User Computing (EUC) architecture).

14. TfL's existing corporate user authentication service (part of the EUC architecture) is sufficient for secure access by TfL staff.

15. External access to the system by 3rd party users will not be required, aside from the potential need for suppliers' access to provide support.

16. The Administrator for CentreComm will be fulfilled by a CentreComm role.

17. Incident management fits within the TfL Technical Reference Architecture model as follows; Application Reference Architecture: Transport Operations: Incident Management. GIS is within Information Asset Management.

18. The service will be hosted internally to TfL.

19. Google Earth will be available via TfL internet access for street view, sometimes required when a driver can only provide visual cues for their location.

20. A radio call lasts 90 seconds then the call drops automatically. This is an iBus restriction. If the CentreComm operator needs to continue speaking to the driver after 90 seconds they will call the driver back. All radio calls are limited to 90 seconds apart from incoming code red calls that are answered within 60 seconds, those last for up to 13 minutes.

Transport for London

2.7. Safety and Security Profile

Incident management systems in LUCC and CentreComm;

a) Are not safety critical. The control centres can continue to perform their role if the incident logging is temporarily not available, revert to paper notebooks for logging their actions and decisions, see AR-04.

b) Have a low tolerance for data loss in the event of a system failure see AR-05.

c) Have data held with a TfL information classification standard of

a. TfL_RESTRICTED Part 2, except for

b. Contingency Plans which are considered TfL _Confidential (ref 2)

d) There is no requirement for any higher level of classification beyond TfL classifications; operational Contingency Plans need to be available to LU staff to be read and understood prior to an incident so therefore cannot have very restricted access, they are operational documents. They may be developed from other, more restricted plans from other agencies. For example, for a state funeral, these types of strategic plans are out of scope for an operational incident management system and are managed separately.

Information sent out on the SMS and Email is TfL_RESTRICTED Part 1, it is intended for distribution to a wide TfL and partners' audience.

Information sent out on the Bulletin Board is TfL_Restricted Part 1; it is directed at bus operators' behaviour, and may involve staff planning, for example in case of a diversion.

The Live Information Desk provides public facing TfL_UNCLASSIFIED information.

Emergency alerts (currently SIMlink):

a) Are not safety critical, the ability to communicate with the Line Control Centres and other control centres in an emergency if SIMlink (which is currently delivered via the LU domain network) can be fulfilled via telephone or Connect radio in the event of SIMlink not being available.

b) Are currently provided via the TfL network infrastructure.

Transport for London

3. System Context

3.1. Use Case

The diagram below shows the main functions within and interfacing to the system and the actors that interact with them.

Fig 3. High level use case

Transport for London

The high level functions the solution will deliver are:

- **Create incident / event** – allows the user to manage (i.e. create and update) incident details

    o When an Operator selects an Incident Type, a standard Action List may optionally be mapped to the incident to guide an Operator through the standard actions for the incident type. An incident dash-board will report the completion status of each item on the action list,

    o An Operator can select an Incident Activity Template, which provides templates for common activities performed by the LUCC. (Centrecomm have indicated they would not use the template / Proforma function initially. Their response plans tend to be less complex.)

- **Enable GiS mapping** - of incidents, events and Contingency Plans

- **Maintain Desk Log** – The Desk Log enables users to records any activity taking place in a Control Centre that does not merit a separate incident entry

- **Create alert** – allows the Operator at the LUCC to send an alert in an emergency, and for recipients to acknowledge receipt

- **Broadcast incident and service status message** – of incident progress or service status

- **Create Weather Readiness Plans** – allows the user to create a Weather Readiness Plan and to maintain the status and report on progress, depending on access rights

- **Manage Contingency Plan** – enable LUCC to create, view and manage a Contingency Plan to be invoked depending on event or incident types

- **Admin maintenance of action lists** – to implement the IMPULSE response plan approach, create Weather Readiness Plan and Contingency Plans

- **Flexible Visibility of Incidents** via Role Type

- **Reporting –** Allows users to query and report on Incidents, depending on access rights.

3.2. Role Types

Role	Access type	Organisation location	Solution interaction	User Volumes
Operator	Full functionality	Within the Control centre	Log and manage Incidents Add to Desk Log Send SMS/ email messages Centrecomm only; Publish to Bulletin Board Create and update Diversions, Logs and Ticket Requests. Assign and de-assign Resources from Incidents and Log on/off Resources onto Duties.	50 LU + 25 CC

Transport for London

Role	Access type	Organisation location	Solution interaction	User Volumes
Operator –Alert	Full functionality	Within the Control centre	Send emergency alerts - LUCC	10
Administrator	Full functionality	Within the Control Centre	Manage templates and user profiles Maintain Reference Data (e.g. Incident Cause Codes, Duties) Manage User access and permissions. An 'Admin' user has all the permissions of an Operator.	2/3
Emergency Alert Recipient	Alert receipt to I/P address	Line control centres, TACC, PCR, BTP	Receive alerts – no log in required	15
Weather Readiness Reporter	Limited functionality – Web / mobile	Service Control Managers across TfL	Update status on Weather Readiness Plan	100
TfL Staff – read only	Read only web / mobile	Across TfL	Browse incident detail Browse Dashboard	100+
Contingency Planner	Limited functionality	Within Network Operations and Control	Create contingency plans and Weather readiness plans	10
Live Information Desk (LID) Operators	Limited functionality	Within the Control Centre	View incidents and create and append a LID Desk Log with details of communication sent out.	10
Communication Recipient	n/a	Across TfL and partner organisations (40 bus operators 100/200 service controllers at each operator, support contractors)	Receive incident progress and service status; SMS/Email Message Bulletin Board – log in required for Bulletin Board	4,000
Performance metrics analyst	Limited functionality	Within the Control Centre	Report and analysis of Cat one incidents, incident start-end stats Call behaviour	2/ 3

Transport for London

An Operator in a Control Centre can be as follows;

For CentreComm;

- ERT – Emergency Response Team (Radio Desk Operators)

- NRT – Network Response Team

- NDM – Network Duty Manager

- CentreComm Management

For LUCC;

- Incident Desk Controller

- NOM - Network Operations Managers (can also send Emergency Alert)

- NIM - Network Information Managers (can also send Emergency Alert)

- NOC - Network Operations Controllers (can also send Emergency Alert)

- SOO - Senior Operating Officer

- DOME - Duty Operations Manager Engineering

- DOE - Duty Operations Engineer

Transport for London

4. Functional Requirements

Requirements are prioritised using the MoSCoW method:

- **M** – MUST: Describes a requirement that must be satisfied for the solution to be considered a success.

- **S** – SHOULD: Represents a high-priority item that should be included in the solution if it is possible. This is often a critical requirement but one which can be satisfied in other ways if strictly necessary.

- **C** – COULD: Describes a requirement which is considered desirable but not necessary. This will be included if time and resources permit.

- **W** – WON'T: Represents a requirement that stakeholders have agreed will not be implemented in a given release, but may be considered for the future.

Ref	Description of Requirement	Priority

4.1. Manage Incident / Event UC01

Both control centres respond to an Incident;

- LUCC respond to incidents escalated to them by the Lines or by the emergency services,

- CentreComm respond to incidents radioed in by bus drivers and from multiple other sources such as Police etc.

Create incident **IN-01**	The solution must enable a user to create and update an Incident. See Section 7 for a list of attributes.	Must
Create incident **IN-02**	The solution must generate and display the Incident Reference Number upon the creation of a new Incident, see section 7 for data description. This shortened (3 digit max 4 digit) Incident Reference Number is used for communication with third parties and is different to the Unique ID (IN-03) which is the solution's internal reference number for a saved incident.	Must

Transport for London

Ref	Description of Requirement	Priority
Create incident **IN-03**	The solution shall generate a unique ID for the incident upon saving the Incident (i.e. when the Incident is committed).	Must
Create incident fast **IN-04**	The solution shall facilitate keyboard short-cuts (ideally specified by TfL) to allow a user to undertake common tasks, including but not limited to: create an incident, save an Incident. The intent of this is to be able to retain similar short-cuts to reduce training needs for operations staff.	Must
Action list IN-06	The solution shall enable an Action List to be associated with an Incident, dependent on the Incident Type.	Must
Add Incident Activity **IN-07**	The solution shall enable a user to add an Incident Activity to an Incident using an Incident Activity Template.	Must
Add Incident Activity **IN-08**	The solution shall enable a user to add one or more Incident Activities to an Incident as free text fields.	Must
Concurrent updates **IN-09**	The solution shall allow multiple Incident Activities to be added to an Incident concurrently by multiple users.	Must

Transport for London

Ref	Description of Requirement	Priority
Alert of concurrent activity **IN-10**	The solution shall indicate to a user editing an Incident, when that Incident is concurrently being edited by another user; showing i) user details and ii) area being edited (if applicable). .	Must
View audit trail **IN-11**	The solution shall make the audit trail available to be viewed as part of the Incident.	Must
Limited visibility **IN-12**	The solution shall enable a user to set Visibility of an Incident. (For example, Incidents created by Network Operations Managers are not visible to any other Role Type)	Must
Multiple Incidents **IN-13**	The solution shall enable a user to update multiple Incidents simultaneously i.e. users must be able to open multiple Incident screens to create a new Incident or update existing Incidents. See IN-14	Must
Multiple Incidents limit IN-14	The solution shall allow a configurable limit to be set for the number of incidents to be open concurrently for updating.	Should
Incident status IN-15	The solution shall enable a user set an Incident's status. See Section 7 for status detail.	Must
Incident Status IN-16	The solution shall enable an incident to be managed through a lifecycle, via the statuses described in Section 7.	Must

Transport for London

Ref	Description of Requirement	Priority
Incident status IN-17	The solution shall enable an Incident Status to be displayed with a colour coding scheme.	Must
Incident status **IN-18**	The solution shall enable a user to set an incident to Closed within the Incident creation process (i.e. without having to save first). See also INU-06.	Must
Incident status – closure **IN-19**	On closure of an Incident, the solution shall prompt a user with a default closure activity checklist based on the actions previously taken for the Incident. For example, if a Bulletin Board has been previously sent to notify a diversion, offer a default "Diversion cleared" message to be sent to the same recipient group.	Should
Incident status – closure **IN-20**	The solution shall offer the user the option of editing a default message offered by the closure activity checklist before sending.	Should
Clear linked incidents IN-21	When an Incident is closed, the solution shall provide the user with the option of also closing a Linked Incident. See also, section on Link Incident 4.3 below.	Must
Re-Open Incident IN-22	The solution shall allow a user to re-open a closed Incident to allow further updates to be made.	Must

Transport for London

Ref	Description of Requirement	Priority
Incident Queue **IN-23**	The solution shall enable presentation of Incidents, in an Incident Queue; including but not limited to; • NRT list, CentreComm incident assigned to the NRT for follow up, • NOM list, LUCC incident assigned to the NOM for review and closure.	Must
Queue Refresh Frequency IN-24	The solution must ensure an Incident Queue must refresh at least once every 30 seconds, at a frequency that ensures the user has a current view of all records (Incidents, Events etc),	Must
Share incident **IN-25**	The Solution shall not, within its initial design, enable a control centre to make their incidents directly visible to another control centre. To clarify - LUCC do not currently wish to have CentreComm users directly access their incident data - and vice versa.	Won't
Create dashboard incident **IN-26**	The solution shall enable a user to create an entry on a (separate) Dashboard that is unrelated to either Control Centre's incidents (and one that can be published for recipients that do not require login-based access to the solution	Could

4.1.1. Manage Incident – LUCC specific requirements

LUCC will create an Event for planned activity, either on the LU network or in the LUCC. An Event has similar data attributes to an Incident.

| Attach files INU-01 | The solution shall enable a user to attach and remove one or more files to an Incident.
For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm | Must |

Transport for London

Ref	Description of Requirement	Priority
View attachment **INU-02**	The solution shall enable a user to view the content of an attached file. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Create event **INU—03**	The solution shall enable a user to manage (i.e. create and amend) an Event. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Location details **INU-04**	The solution shall allow a user to link through to the Location Directory for the location specified for the incident For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should
Category incident **INU-05**	The solution shall enable an authorised user to manage the CAT 1 status of an Incident. This will support performance analysis. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Incident closure **INU-06**	The solution shall restrict access to the ability to close an Incident by Role Type, e.g. only the NOM can close an Incident in the LUCC. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

4.1.2.Manage Incident – CentreComm-specific requirements

Ref	Description of Requirement	Priority
Handover Incident **INC-01**	The solution shall enable an authorised user to assign Incidents to an Incident Queue in real-time e.g. by setting a Status of an Incident to NRT. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
De-assign Incident **INC-02**	When an Incident is cleared, the solution shall automatically de-assign any Resources that have been assigned to the Incident. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Diversions on Route **INC-03**	When a new Incident is created, the solution shall indicate whether a Diversion is currently in place for the selected Bus Route. For the avoidance of doubt this requirement shall not apply to the LUCC DC. .	Must
Diversions on Route **INC-04**	When a new Incident is created and a Diversion is currently in place for the selected Bus Route, the solution shall provide a visual indicator to the user to allow them to open the Diversion for reference purposes. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
4.2. Incidents and Events: Link Incident UC01.1 Scenarios: • An Incident is **duplicated**, e.g. multiple calls may be received from bus drivers relating to delays caused by an accident along a Bus Route, could be upward of 20 Incidents raised • Separate Incidents are **linked**, e.g. stone throwing at a number of buses that each sustain some damage, where a single police response is made • Referencing a **previous** Incident supports incident response based on previous incidents, e.g. signal failures at Colindale, incidents involving 22 points at Edgware Road, bridge strikes at HC3, failures of lift 2 at Elephant & Castle.		
Candidate incidents **LI-01**	When an Incident is created, the solution must evaluate whether there are related Incidents according to configurable matching criteria, including but not limited to: • Status (e.g. Open) • Location • Street Name • Junction • Incident type • Bus Route • Running Number • Date created (within a user-configurable date period) • Time (within a user-configurable time period)	Must

Transport for London

Ref	Description of Requirement	Priority
Previous incidents LI-02	The list of any related incidents found shall be presented in a format that allows the user to distinguish between them and identify suitably related incidents. LU scenario, to support incident response based on previous incidents, e.g. signal failures at Colindale, bridge strikes at HC3, failures of lift 2 at Elephant & Castle. CentreComm Scenario; Stone throwing at a junction.	Must
Previous incidents LI-03	The solution shall allow the Operator to open an Incident from the list presented.	Must
Offer candidates LI-04	The solution shall offer existing Incidents that match the criteria of the current Incident being created as Candidate Incidents for linking to the current Incident.	Must
Link incidents LI-05	The solution shall enable a user to link Incidents.	Must
Merge duplicates LI-06	The solution should enable a user to nominate a lead Incident in linked Incidents.	Should
Merge duplicates LI-07	The solution shall enable a user merge all activity logged against all linked Incidents into a single lead Incident.	Should

Transport for London

Ref	Description of Requirement	Priority
Open Candidate **LI-08**	The solution shall allow Candidate Incidents to be re-opened by a simple screen function, e.g. double clicking with a mouse from the list of Candidate Incidents.	Should

4.3. Incidents and Events: Manage Desk Log UC05

A Control Centre will record any activity or information within the control centre that does not merit creation of a separate incident entry on a Desk Log, e.g.:

- CentreComm: staff booking on and off shift, calling in sick (created Daily)

- CentreComm LIDs (Live Information Desk) outbound comms published (created Daily)

- LUCC: non-incident specific messages sent out on Network status, exceptions in the staff taxi activity (created Monthly)

Ref	Description of Requirement	Priority
Create Desk Log **DL-01**	The solution shall enable the user to manage i.e. create and append to a Desk Log.	Must
Preserve Desk Log **DL-02**	The solution shall allow a Desk Log audit trail to be accessible to the user.	Must
Log View **DL-03**	The solution shall provide a means for the user to search for and view a Desk Log including but not limited to keyword searches and filtering. (See also Search and Filter section)	Must
Log View **DL-04**	The solution shall provide a means for the user to search within a Desk Log including but not limited to a keyword search. (See also Search and Filter section)	Must

Transport for London

Ref	Description of Requirement	Priority
Limit visibility **DL-05**	The solution shall enable the user to set a Desk Log entry to limited visibility to a group of users.	Must
Audit trail **DL-06**	The solution shall retain an audit trail of all updates made to a Desk Log entry.	Must

4.4. Incidents and Events: Manage Diversions – CentreComm only UC08

CentreComm will decide to implement a Diversion, i.e. a change to a bus route (or routes) if an incident or event impacts the running of the bus network. It will be implemented for a period of time by the bus operators. The Diversion Reference Number is shared with bus operators and is used as a reference between the bus operator and TfL when bus operators report lost miles due to a Diversion.

The purpose of recording the diversion is to;

- Record Diversion Reference Number,

- Have visibility of diversions in force when calls come in,

- Notify the Bus Operators of the diversion, via the Bulletin Boardand SMS/ Email Message.

Ref	Description of Requirement	Priority
Create Diversion **DV-01**	The solution shall allow Network Response Team (NRT) operators to create and update Diversions when creating or updating and Incident. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Copy Diversion **DV-02**	The solution mushallst allow an existing Diversion to be copied to create a new Diversion that can be edited and saved as a new Diversion. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Visual Mapping **DV-03**	The location of a Diversion shall be automatically displayed on the map via a graphical icon / image. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Clear Diversion **DV-04**	The solution shall allow a Diversion to be set to a Status of Cleared. Note: A Diversion will have two Statuses: Open or Cleared. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Clear Diversion **DV-05**	When Diversion is Cleared, the solution shall offer Incidents, that are linked to that Diversion, to be cleared. Note: Conversely, when an Incident is Cleared, any associated Diversion must not be Cleared. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Diversion List View **DV-06**	The solution shall allow a user to view a list of Open and Cleared Diversions via the NRT view. By default the Diversion list must be displayed in order of created date and time. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Diversion List View **DV-07**	The solution shall allow filters and sorts to be applied the Diversion list (for example by affected Route). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Diversion Updates **DV-08**	The solution shall ensure that when a Diversion is open for update by a User, other Users should be prevented from editing the Diversion until the Diversion is saved and closed by the first User. In this scenario, details of the user performing the update must be displayed For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Audit History **DV-09**	The solution shall ensure that, when a Diversion is saved, users can view the Diversion update history. For the avoidance of doubt this requirement shall not apply to the LUCC DC. .	Must
Re-Open Diversion **DV-10**	The solution shall allow a Diversion that is set to Cleared to be re-opened to enable the diversion to be reinstated (and updated as necessary). When a Diversion is re-opened it must be set to the default Status of Open. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Update Cleared Diversion **DV-11**	The solution shall allow a Diversion that is set to Cleared to be updated as necessary without being re-opened e.g. in the scenario where missing information should be added to a cleared diversion For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Linked Incident Diversions **DV-12**	When more than one Incident are linked, any Diversions assigned to one of the linked Incident shall also be associated to other linked Incidents. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
4.5. Incidents and Events: Manage Ticket (Holder) Request – CentreComm only UC07 Surface Transport Operations may decide to accept tickets from alternative transport providers (Train Operating Companies) where there has been a disruption to their services. Centrecomm; • Send the Ticket Request Pre-Pay Number to the bus operators (and bus drivers on request) for bus driver to enter into their ticket machines, • Report on the number of ticket requests made from other transport providers on a periodic basis.		
Record Ticket Requests **TR-01**	The solution shall enable the User to create an in-bound Ticket Holder request from different sources (e.g. LU, Train Operating Companies (TOC)), see section 7 for data descriptions. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Ticket Request Expiry **TR-02**	The solution shall automatically expire / clear Ticket Requests at midnight (2400hrs) on the day of creation unless a later date and time has been set for "valid time off". For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Pre-Pay Number **TR-03**	The solution shall automatically generate and present a Ticket Request Pre-Pay Number to the user on creation of a new in-bound Ticket Request. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
External Publish **TR-04**	The solution shall allow Ticket Requests to be published to an external Bulletin Board. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
Publish to SMS **TR-05**	The solution shall allow a Ticket Request to be published via SMS /Email Message. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Ticket Request List **TR-06**	The solution shall display a list of current and recently cleared Ticket Requests, by default the list must be displayed in order of last update / create date and time. It shall also be possible to apply other filters and sorts to the list (for example by affected Route). For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Clear Ticket Request TR-07	The solution shall allow a user to update and Clear a Ticket Request, including prior to the specified "valid time off" date / time. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Clear Ticket Request **TR-08**	On clearing of a Ticket Request, the solution shall prompt a user with a default closure activity checklist based on the actions previously taken. For example, if a Bulletin Board has been previously sent to notify a Ticket Request, offer a default "Ticket Request cleared" message to be sent to the same Recipient List. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should
Status TR-09	The solution must be able to record the status of a Ticket Request as either "OPEN" or "CLEARED". For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
4.6. Incidents and Events: Manage Notice of Events – CentreComm only UC06		
Events are a planned occurrence that impact on the road network in some way, that may cause a planned Diversion. It could be a bus-stop closure or just notice that there may be delays. They are logged as a Notice of Event (NOE) by Area Managers, a large percentage of NOE's do have bus Diversions associated with them that are textually described on the NOE.		
NOE Import **NE-01**	The solution shall import Notice of Event (NOE) data from a TfL source system, (currently a SharePoint solution). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Visual Mapping **NE-02**	The location of a NOE, once imported, shall be automatically displayed on the map via a graphical icon / image, if sufficient geo-coding info is available. Note: An NOE's location is expected to be defined by reference to a Bus Stop. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Visual Mapping **NE-03**	The solution shall display relevant NOEs on the map when the current date falls between the NOE start and end date, as a default. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Search for NOEs **NE-04**	The solution shall enable a filtered search for future or past NOE's and result to be displayed on a map by date range. For example, an operator may wish to see NOE's on the map commencing at a point in the future. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could

Transport for London

Ref	Description of Requirement	Priority
NOE Map View **NE-05**	When displaying NOE icons on the map, two layers shall be available to distinguish those NOEs where a Diversion is required, and those where a Diversion is not required. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Event List View **NE-06**	The solution shall allow NOEs to be viewed in a tabular list format. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Event Calendar **NE-07**	The solution shall allow NOEs to be viewed in a calendar / diary type view. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could

Transport for London

Ref	Description of Requirement	Priority
4.7. Incidents and Events: Manage Weather Readiness Plans – LUCC only UC09		

A Weather Readiness Plan holds a series of action lists presented in a "54321" format i.e. Day 5 is 4 days before the expected onset of a weather event, with preparation activities, responsible parties. This is repeated for Day 4, Day 3 Day 2 and Day 1. It is generally initiated on Day 5, i.e. 4 days prior to expected arrival of weather. Day 1 being the day the weather is expected to arrive.

On a plan being triggered, each line or business area with responsibility for a plan completes their status each day. This is summarised and reported by the LUCC.

The activities on a Weather Readiness Plan for a line / dept for an area (i.e. stations, trains & service control and maintenance) will be defined as Action Lists.

Weather Readiness is reported in a hierarchy;

- Each line's / dept status for:

- Stations, Lines and, Service control and maintenance

In addition depts. (e.g. NOM/ SOO Asset Performance) report on; Staff welfare, Communications, for a series or action list of tasks entered by the responsible user. The status is rolled up to;

- a line status, then,

- a network status,

only showing green when all components are green. This enables the LUCC to identify where action is outstanding.

Transport for London

Ref	Description of Requirement	Priority
Create checklist template **WP-01**	The solution shall allow the admin user to create a Weather Readiness checklist template that enables actions and status of action to be recorded for each line for; • stations, • trains, • service control and maintenance, for several days (currently but not limited to 5,4,3,2,1) leading up to a weather event. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Should
Record status **WP-02**	The solution shall enable the Weather Readiness Reporter to record status against the weather plan. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Should
Report readiness status **WP-03**	The solution shall enable the Weather Readiness Reporter to report on all lines status with regard to Weather Readiness in a summary for print or viewing. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Should
Assign weather plan **WP-04**	The solution should allow an administrator to assign responsibility for completing a weather readiness action list to a Weather Readiness Reporter. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Should
Invoke weather readiness **WP-05**	The solution shall allow the User to invoke a Weather Readiness Plan, notifying the responsible parties, indicating which Day is being invoked for the Weather Readiness Plan. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Should

Transport for London

Ref	Description of Requirement	Priority
4.8. Incidents and Events: Manage Contingency Plans – LUCC only UC10 Contingency Plans hold a series of steps or activities with activities listed, with a responsible party. A Contingency Plan can be invoked by; • an unplanned incident or an unplanned event, or • a planned event or series of events, e.g. there is a Wembley event plan that is invoked for each event at Wembley.		
Create Contingency Plan **CP-01**	The solution shall allow the user to create a Contingency Plan. This may include; • Textual description of the Contingency Plan, • Action List to be completed when the Contingency Plan is invoked, • Pictures to be referenced when a Contingency Plan is invoked, • GIS map(s) to be referenced when a Contingency Plan is invoked. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Could
Invoke Contingency Plan **CP-02**	The solution shall allow the user to invoke a Contingency Plan by associating it with an incident or Event. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Could

Ref	Description of Requirement	Priority

Transport for London

Ref	Description of Requirement	Priority
4.9. Geo-code Incident UC01.2		
Geo-code incident **GI-01**	The solution shall enable the location of an Incident to be geo-coded. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Map Location **GI-02**	The solution shall enable an Incident location to be displayed on a map (including during creation of an incident) For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Map Location **GI-03**	The solution shall enable an Event location to be displayed on a map, where appropriate. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Street Search **GI-04**	The solution shall provide a user with a street search function to locate specific streets within the Map Extents. This requirement must be considered in conjunction with INC-01 and INC-02a; a bus route will provide an initial filter for streets. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Street Search result **GI-05**	The solution shall present the following information in a street search result set to help identify the required location: • Street Name, • Borough, • Postal Area Code. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
Street Search Highlight **GI-06**	The solution shall display a street search result in the centre of the screen with a visible highlight to aid the user in locating the street on the map. Note: the highlight may take the form of a marker placed on the street at its mid-point or the street may be highlighted. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Layer info on map **GI-07**	The solution shall enable the user to select a layer of information to be displayed on a map as icons, e.g. bus diversions. See Section 7 for layers and data sources. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Layer info on map **GI-08**	The solution shall enable the user to select multiple layers of information to be displayed on a map as icons, e.g. bus diversions. See Section 7 for layers and data sources. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Detail on map info **GI-09**	The solution shall allow an icon for all geo-locatable data types (e.g. Incident, Event, Diversion, signals etc) to be selected and for summary info to be presented to the user, see section 7 for detail. For example, on clicking a resource Icon the solution must display the resource name, Mobile Number, Duty, and Assigned Incidents. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
Two mapping products **GI-10**	The solution shall offer at least two mapping products for user selection, in order to complement and cover off the limitations of different products. Acceptable product include; • Ordnance Survey MasterMap detail, • Ordnance Survey Address point detail, • Ordnance Survey Street View raster mapping detail, • ITN RRI (Route Routing Information) • Collin Bartholomew, • A to Z detailed For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Base Maps **GI-11**	The solution shall provide a consistent base map layer as the User zooms in and out of the map. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Base Map – detail **GI-12**	The solution shall provide sufficient detail at the highest magnification to show building outlines and building numbers to aid the accurate locating of Incidents. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
Define the Map Extent **GI-13**	The solution shall provide map coverage for the Map Extent, note this is largely but not entirely within the M25 boundary. This is to ensure all current London Bus Routes and suburban services are visible. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Draw impact zone - circular **GI-14**	The solution shall allow a user to draw a circular exclusion zone or cordon from a point, dynamically displaying the depth of the exclusion zone in metres. To function in conjunction with GI-16. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Draw impact zone - polygon **GI-15**	The solution shall enable the user to draw an impact area (e.g. for a contingency plan) on a map, and retain the geo-co-ordinates, for example using a polygon To function in conjunction with GI-16. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should
Save impact zone **GI-16**	The solution shall enable the user to save the geo-co-ordinates, of a drawn area as an attribute of the related incident or event. To function in conjunction with GI-14 and GI-15. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should

Transport for London

Ref	Description of Requirement	Priority
4.9.1.Geo-code Incident CentreComm-specific requirements		
Street search result **GIC-01**	The solution shall return the search result screen to the default map resolution set for the User. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Could
Default Map **GIC-02**	The solution shall allow a user to set a preferred default map resolution, i.e.to set the default magnification level that the map should use when switching to display a new map for an Incident, Event or Diversion. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Default Map Type GIC-03	The solution shall allow a user to set the default map type from the mapping solutions available in requirement in GI-12. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Could
Street Selection **GIC-04**	When locating an Incident, the solution must present a list of streets relating to the Bus Route entered. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Street Selection **GIC-05**	The solution shall enable a user to select a street, on selection; the solution must display the required street on the map. See also GI-06. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority
Street Location **GIC-06**	When locating an Incident, the solution shall allow a street name to be searched that may not be on the normal Line of Route for the Bus Route (e.g. if the bus is on Diversion). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Street selection **GIC-07**	The solution shall offer a predict facility when the user is entering a street name, initially limited to the street names on the bus route, otherwise all matching street names in the Map Extent. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should
Junction search **GIC-08**	The solution shall enable the user to perform a road junction search. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Should
Ref	Description of Requirement	Priority

Transport for London

Ref	Description of Requirement	Priority
4.10.	**Outbound Communications**	
Integration with three communication channels is required: • SMS / Email Message to specified stakeholder message groups. For third parties, e.g. bus operators this can be a prompt to check the full communication on the Broadcast, • Publish to a "Bulletin Board": accessible via a user name and password combination, • Emergency Alert to a dedicated terminal.		
4.10.1. Send SMS / Email Message UC02.1 CentreComm need to update the Bus operators and other TfL stakeholders on the status of incidents, diversion and ticket requests. LUCC need to update TfL staff and other stakeholders on service disruptions and incidents. SMS / Email messages are sent to pre-defined Recipient Lists e.g. senior management, line controllers, LIS (Line Information Specialists etc.) for example; • Service Status Messages, are sent out at start of traffic, on the hour and at close of traffic confirming the status across the network, these messages are TfL_UNCLASSIFIED, • In the event of a wheel-stop incident a message is sent out every 10 minutes updating the status of the delay, • Notifying the progress of an incident, • Update the Bus operators and other TfL stakeholders on the status of incidents, diversion and ticket requests.		
Create message **MS-01**	The solution shall enable the User to create an SMS / Email Message via SMS integration using SOAP/ XML protocol, see Ref 11.	Must

Transport for London

Ref	Description of Requirement	Priority
Broadcast for incident **MS-02**	The solution shall enable a user to create an SMS / Email Message associated with an Incident, and retain the details as an Incident Activity. The message text could be based on a message text previously sent associated with the Incident.	Must
Guaranteed send **MS-03**	The solution shall provide a message delivery to at least the same level as the SMS and Email service currently provided by PageOne. Note as the email / text service is dependent on third party public networks, there are no SLAs associated with this service. This requirement is intended to ensure that implementing an API to the messaging service does not reduce the performance in terms of speed of delivery and resilience that the current mechanism currently delivers.	Must
Flag event **MS-04**	The solution shall enable a user to send out an SMS / Email Message to a Recipient or Recipient Group associated with an Event, e.g. when the date or time of an event is approaching.	Must
Message Template **MS-05**	The solution shall enable an authorised user to create an SMS/ Email Message Template.	Must
Draft message MS-06	The solution shall compose a proposed SMS/email Message based on the characteristics of an Incident and offer to the User, e.g. when a Person under a train, always send a series of texts.	Should
Scheduled messages **MS-07**	The solution shall be configured to send out a scheduled SMS/ Email Message confirming status across the network. Scenario; the NIM sends an hourly status message, could prompt for this.	Could

Transport for London

Ref	Description of Requirement	Priority
Message tag **MS-08**	The solution shall be configured to enable an SMS/ Email Message to be tagged to be relevant to specified Recipient List(s). Scenario: an Incident Type or Location triggers a draft message to a recipient Group or groups	Won't
4.10.2. Publish to Bulletin Board– CentreComm only UC02.2 CentreComm require to update the Bus operators and other TfL stakeholders on the status of incidents, diversion and ticket requests. Note, publishers do not require additional access controls, all CentreComm operators will publish to the Bulletin Board.		
External Publish **EP-01**	The solution shall enable the User to publish information to an external-facing Bulletin Board in real time. Note: CentreComm currently publish information to a Blog (currently hosted on Google BlogSpot). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Update External Publish EP-02	The solution shall allow the User to update published information on the Bulletin Board, e.g. where the status of an incident changes, the original statement can be amended. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Audit history EP-03	All updates and new content to the Bulletin Board shall be recorded, and the audit trail available to view. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Access Control to Bulletin Board **EP-04**	The solution shall ensure that access to the Bulletin Board is subject to access control with only authorised Communication Recipients able to view the published information. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Audit logins **EP-05**	The solution shall record all logins and attempted logins to the Bulletin Board. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
4.10.3. Create Emergency Alerts (SIMlink replacement) – LUCC only UC02.3 This is a real-time communication between a sender and one or many dedicated terminals to alert other control centres of an emergency. Note these are all situated in secure control centres.	
Send alert **EA-01**	The solution must enable an authorised user (see EA-08 below**)** to send an Emergency Alert to one or many recipients or Recipient Lists on dedicated terminals. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Receive alert **EA-02**	The solution shall allow the alert recipient functionality to be made on always-on workstations (which currently use generic Line Control Centre-level logins, have specific I/P addresses), i.e. the message must be seen and acknowledged. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Alert status **EA-03**	The solution shall notify the user of the receipt status of the alert. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Ack alert EA-04	The solution shall enable the recipient (the user of the dedicated terminal) to acknowledge that they have received the alert. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Manage recipients EA-05	The solution must enable the User to manage (i.e. create, update and delete) the group of alert recipients. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Alert templates EA-06	The solution shall enable the authorised User to create alert templates. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
Control access EA-07	The solution shall enable business rules to be defined against a template (e.g. only users with a particular role can send alerts using a specified template). For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Must
	4.11. Reporting and Search: Search and Filter UC03	
Search within incident SF-01	The solution shall enable the User to search within an Incident on all data captured, using multiple search criteria including but not limited to name, abbreviation, and short code.	Must
Wild card search SF-02	The solution shall enable the User to search on any field using wild cards.	Must
View with filters SF-03	The solution shall enable the User to view incidents using filters including but not limited to status, location, date.	Must

Transport for London

Ref	Description of Requirement	Priority
Search linked incidents SF-04	The solution shall enable the User to search and view Linked Incidents.	Must
'A' Road Searches **SF-05**	The solution shall enable the User to search for a street by the 'A' road number.	Must
Migrated Incident Data SF-06	The solution shall enable the User to search historic Incident data migrated from the legacy system.	Must
Search interface **SF-07**	The solution shall enable the user to search using the same "look and feel" as the interface used to enter each data type (e.g. Incident, Diversion).	Must
Default Search criteria **SF-08**	The solution shall enable the user to default search criteria to a configurable "same day" search result if no explicit date or time criteria are specified e.g.; • from 00:00 on the current date for CentreComm, • from 4.30 for the "start of traffic" day for LUCC.	Must

Transport for London

Ref	Description of Requirement	Priority
Look up reference data **SF-09**	The solution shall enable the reference data, see Section 7, to be searched, including but not limited to: • Bus Stop Data – User enters a valid Bus Stop number • Bus Shelter – User enters a valid Bus Stop number • Bus Route Streets (Out and Back Route) – User enters a valid Bus Route • Bus Route Turning Points - User enters a valid Bus Route • Operating Garage – User enters a route (enables operator to call garage if necessary) • Location detail –User enters a valid Location	Must
Links to websites **SF-10**	The solution shall provide a configurable menu with links to commonly used web sites.	Should
4.11.1. Search and Filter – CentreComm only		
Migrated Diversion Data Search **SFC-01**	The solution shall enable the User to search historic Diversion data migrated from the legacy system. For the avoidance of doubt this requirement shall not apply to the LUCC DC. .	Must
Filter by Type **SFC-02**	Where relevant, if multiple types (e.g. Incidents, Events, Diversions) are listed on a single screen, the solution shall provide filter by types to allow the User to filter those entry types that are relevant (e.g. to filter the list to show only Incidents). For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

Transport for London

Ref	Description of Requirement	Priority

	4.12. Reporting and Search: Reporting and Analysis UC04
	
	The users require a simple reporting interface embedded in the solution that enables basic reports to be configured and produced, see Ref 13 for examples, e.g,
	
	• the CentreComm manager look at daily and weekly reports for incident trends, call handling statistics.
	
	• reporting from the LUCC falls into the following areas;
	
	    o Access to progress of an incident as it unfolds, currently provided by read-only access to NIMROD or PageOne updates sent out by LUCC,
	
	    o Ad-hoc queries on incidents by the LUCC. Historical data will be available for a minimum of 7 years.
	
	Integration with an industry standard business intelligence tool is also required for complex reporting, see RP-11.	

Define Report **RP-01**	The solution shall enable a user to create reports, see Ref 13, for examples illustrating types of report TfL users expect to be able to produce.	Must
Define Report **RP-02**	The solution shall enable a user to define a set of criteria for a report, using a query builder, including but not limited to: • Data fields to be included, • date ranges, • completion status of incidents.	Must
Define Report **RP-03**	The solution shall enable a user to format a report including but not limited to: • adjust page layouts • add page headers and footers • apply page breaks • add fields • remove fields • add free text • format field descriptions.	Must

Transport for London

Ref	Description of Requirement	Priority
Define Report RP-04	The solution shall enable a user to view a report output.	Must
Define Report RP-05	The solution shall enable a user to print a report output to standard print facilities accessible from MS Windows.	Must
Define Report RP-06	The solution shall enable a user to export a report output to files in ASCII Comma Separated Variable Text (.csv) format.	Must
Define report RP-07	The solution shall enable a user to export a report output to Microsoft Excel (.xls/xlsx) format. For example, desk performance analysis requires number of incidents handled and type of incident handled by user in excel.	Must
Define report RP-08	The solution shall enable a user to export a report output to Microsoft Word format. This will enable further editing; e.g. Incidents reported on several reports will be manually re-worded to ensure appropriate terminology is used before publication.	Must
Define report RP-09	The solution shall enable a user to export a report output to PDF format.	Must
Schedule report RP-10	The solution shall enable a user to schedule pre-defined reports, e.g. daily, weekly, periodic reports.	Must
Export data RP-11	The solution shall have the ability to integrate with industry standard business intelligence tools. (E.g. Crystal Reports, Business Objects, Hyperion)	Must

Transport for London

Ref	Description of Requirement	Priority
Overview Incident Summary RP-12	The solution shall enable display of a high level view Incidents' status to the user on an Incident Summary; in a map or list view with the ability to dynamically link through to Incident or Event detail.	Must
Read only view RP-13	The solution shall enable access to all information in a read-only view e.g. for senior managers to review a full history of an Incident. The only exception to this is where the visibility of the Incident is restricted.	Must
Print incident RP-14	The solution shall enable the user to print Incident details to standard print facilities accessible from MS Windows, e.g as a PDF format.	Must
Mobile access RP-15	The solution shall provide read-only access to Incident details on a mobile device. This would be useful for staff on the ground during a major incident.	Won't
Incident Summary info RP-16	The solution shall enable display of of of a high level view Incidents' status to the user on an Incident Summary, including but not limited to; • Ownership of items on the Action List, • Completion status of items on the Action List, • Incident log summary. This follows on from RP-12	Must

Transport for London

Ref	Description of Requirement	Priority
Performance metrics **RP-17**	The solution shall support reporting of incident progress by providing the ability to analyse incident behaviour, UC-11, for example; • Time to respond to an incident, when is a Cat 1 declared, (see data captured, section 7) • How many Cat 1 incidents on-going at a point in time, (see data captured, section 7) • How long does it take for an incident to move from "Severe Delays" to "Good Service", (see data captured, section 7) • Reports required on weekly, monthly periodic, looking at trends, • Time To Site (TTS) for NIRM, Technical staff and incident channel used, The reporting requirements (see RP-01 and RP-03) provide the capability to create reports, and to extract to a BI reporting tool. The performance metrics analysis will be supported via these capabilities.	Must
Financial periods RP-18	The solution shall enable an incident date to be mapped to a financial period, to support analysis reporting.	Must
Dashboard RP-19	The solution shall allow a Dashboard to accept data from other applications via an open standard interface. This enables the control centre to publish a view of activity beyond their own control centre.	Could
Publish dashboard RP-20	The solution shall allow a Dashboard to be published. This enable the control centre to make an overview available to recipients that do not require access to the solution.	Must
Configure dashboard RP-21	The solution shall allow the layout and content of a Dashboard to be configurable.	Could

Transport for London

Ref	Description of Requirement	Priority
Multiple dashboards **RP-22**	The solution shall allow multiple Dashboards to be created and configured.	Must

Ref	Description of Requirement	Priority

Transport for London

Ref	Description of Requirement	Priority

4.13. Manage Resources – CentreComm only UC01.3

Incidents may require a Resource such as a Network Traffic Controller (NTC) to be assigned to support Incident management at the scene.

NTCs are mobile (in van) staff that are assigned to Incidents that require some physical intervention or action. They can be responding to incidents that occur, or be allocated non-urgent tasks that can be done at some point on their shift (e.g repair a bus shelter).

Other resource types may also be assigned such as a Pick Up Truck or Cleaner.

On-street Resources are managed by;

- London being divided into several Regions.

- Each Region has a number of Duties defined, usually by geographic area within the Region, e.g. the "South" Region has "Southwark NTC" defined as a Duty.

- A Duty has several Shifts defined, e.g. "Early turn", Late turn", each has a start time and end time. The Duty has a mobile phone assigned to it that a Resource will pick up when they log onto a Shift.

- A Resource, eg NTS and Bus Station Controllers (BSC) may also have a PDA

Resources may carry two devices;

- A rugged basic mobile phone that they will always carry with them. This device will be used to geo-locate the Resource and is first point of contact for a Resource for CentreComm

- A PDA, functionally-rich device with applications to manage their tasks. This device could be used to exchange messages with CentreComm, eg on the logged –in status of a Resource.

Transport for London

Ref	Description of Requirement	Priority
Assign Resource RS-01	The solution shall allow available Resources e.g. NTCs, to be assigned to Incidents. Note: Multiple Resources may be assigned to an Incident. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Assign Resource **RS-02**	The solution shall allow the user to send an SMS to a Resource with details of the incident assigned, invoking functionality described in MS-01. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Assign Resource **RS-03**	The solution shall offer a default SMS message text for the user to accept or update prior to sending, including but not limited to: • Incident ID • Location • Location description • Incident description For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Assign Resource **RS-04**	The solution shall log all actions performed on a Resource, including the despatch of the SMS, on the audit trail. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Assign Resource **RS-05**	The solution shall allow a Resource to be allocated to multiple Incidents concurrently. This enables the Control Centre to assign a Resource to a non-urgent incident, e.g. repairing a Bus Stop, which they will schedule around responding to more urgent Incidents. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Resource to attach photos **RS-06**	The solution shall not preclude a potential future requirement that allows a Resource to take a photo of an incident and attach it to an incident. This is an element of mobile device integration capability. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Won't
Resource Availability and status – list **RS-07**	The solution shall display the Resources to allow a user to allocate Resources to Incidents on a **list**. Resource details to display, include but are not limited to: a. Type, e.g. NTC b. Location relative to the Incident, the distance away ("crow flies" distance) (see RS-03) c. Logged in status, i.e. Show only logged in resources d. Whether they are available or not For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Resource Availability and status – map **RS-08**	The solution m shall ust display the Resources to allow a user to allocate Resources to Incidents on a **map**. Resource details to display, include but are not limited to: a. Type, e.g. NTC b. Location relative to the Incident, the distance away ("crow flies" distance) c. Logged in status, i.e. Show only logged in resources d. Whether they are available or not For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Locate resource via polling RS-09	The Solution shall enable "On demand" polling of Resources' Duty mobile phones - to enable their location to be identifed. Such "On Demand" polling shall target just the selected Resource(s). (A resource must be associated with an mobile phone to be geo-located.) For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Locate resource via API RS-10	The solution shall enable the location of Resources to be identified by their Duty mobile phones being polled, via an interface to an API. This may be invoked as an alternative to a polling service, in RS-09.	Should
Integration with Mapping Tool RS-11	The solution shall show the location of Resources on a map via an icon or image. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Integration with Mapping Tool RS-12	The solution shall refresh the location of Resources after each location polling cycle (for those logged on to a shift and locatable). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Record Resource Availability **RS-13**	The solution shall enable a user to record the Resource as available or unavailable, during their shift. Currently a Resource will phone into CentreComm to say they are unavailable or available. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Record Resource Availability via device **RS-14**	The solution shall record when a resource is available or unavailable (e.g. on a lunch break) based on messages sent from a device via an API, e.g a browser plug-in. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Could
Show Resource Availability **RS-15**	The solution shall show the location of logged-in Resources regardless of availability (for example when a NTC is on a lunch break). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Resource Assignments **RS-16**	The solution shall display the Incidents that are currently assigned to a Resource e.g. an NTC. Note, this allows the optimum allocation of Resources to be made by a user. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Location Polling **RS-17**	The solution shall update the location of a Resource with the defined polling frequency. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Polling Configuration **RS-18**	The solution shall allow the location status of specific Resources to be suppressed. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Default Mobile Numbers **RS-19**	Each Resource will have a default mobile number that is used when polling their location. The solution shall allow the default number to be temporarily changed by a user for a specific shift or part of shift For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Default Mobile Numbers **RS-20**	Following from RS-19 the default mobile number shall be retained and offered when the Resource next logs on to a Shift. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Location Refresh **RS-21**	Followin on from RS-09 and RS-10, the solution shall allow the location of a Resource to be polled on request. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Resource on duty & shift **RS-22**	The solution shall enable a user to record a Resource as logged on to a Duty and Shift. The NRT resources currently phone into CentreComm when to confirm they are on Duty for a shift. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
Resource off duty & shift **RS-23**	The solution shall enable a user to record a Resource as logged off from a Duty and shift. The NRT resources currently phone into CentreComm when to confirm they are off Duty for a shift. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Resource on shift via device **RS-24**	The solution shall log the Resources coming on Duty and Shift and off Duty and Shift, via a request sent from their PDA device (currently the O2/Cognito PDA). Note this would remove the need for the Resource to call in to be logged on duty. There are 50/60 calls for each Shift change (i.e. 3 times a day to Centrecomm currently). For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Should
Not logged off **RS-24**	The solution shall highlight logged-on Resources that have not logged off within a configurable set time of their Shift end time. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
Not logged on **RS-26**	The solution shall highlight where a Duty and Shift has no Resource logged on within a configurable set time of the Shift start time. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Ref	Description of Requirement	Priority
4.14. Administrator Functions UC12		
The administrator role will be able to maintain the following; reference data values and associated rules and user permissions		
4.14.1. Reference data maintenance UC12.1		
Maintain incident types AF-01	The solution shall enable the Administrator to maintain (i.e. create and amend) reference data values, section 7.1, including but not limited to: Resources, Duties, Regions, and Shifts.	Must
Action list to incident types AF-02	The solution shall enable the Administrator to associate a number of Action List activities with an Incident Type.	Must
Create Incident Activity Template AF-03	The solution m shall ust enable the Administrator to create an Incident Activity Template.	Must
Incident Activity Template to Action list item AF-04	The solution shall enable the Administrator to associate an Incident Activity Template with an Action List entry.	Must

Transport for London

Ref	Description of Requirement	Priority
Action list sequence **AF-05**	The solution shall allow the Administrator to define the sequence in which Action List items are presented for completion of an incident type.	Must
Define Location **AF-06**	The solution must allow the Administrator to create a location (e.g. a landmark).	Must
File to location AF-07	The solution shall enable the Administrator to attach or detach one or more files to a location, e.g. floor plan of a station to allow the LUCC to incident which entrance is relevant.	Must
Link to Location artefacts **AF-08**	The solution shall allow the Administrator to create a link to information about a location, including but not limited to; • Congestion Control Emergency Plans (CCEP), • Local area maps, • Contract information, • Local bus maps, • Strike co-ordination plans. •	Should

Transport for London

Ref	Description of Requirement	Priority
4.14.2. User profile maintenance UC12.2 There is an overlap between CentreComm and LUCC for recipients of SMS; where senior management may receive updates from both control centres. so where an individual requires both, they will have an entry on each control centre's Recipient list in Page One. SMS Recipient Lists will initially be managed separately within the PageOne application as there is currently no API interface to PageOne that enables Recipient List's contents to be imported to PageOne. Initially Communication Recipients will be maintained in the solution only for access to the Bulletin Board.		
Comms recipient **AF-10**	The solution shall enable an Administrator to create and update a Communication Recipient, required initially for Bulletin Board only.	Must
Recipient list **AF-11**	The solution shall enable an Administrator to create and update a Recipient List, required initially for SMS/ emailing only.	Must
Self-registration **AF-12**	The solution shall support self-registration for access to the Bulletin Board (approx 4,000 users, as approx 40 bus operators and 100/200 service controllers for each bus operator). The implication here is that these external users will not require TfL-assisted support other than the provision of user guide material. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Should

Transport for London

Ref	Description of Requirement	Priority
4.14.3. Product configuration TfL business areas will wish to include additional data fields that do not affect logic, without recourse to the supplier.		
Configuration **AF-13**	The solution shall enable an authorised user to create additional data fields, that do not affect business flow, without recourse to the supplier.	Must
Configure **Map Extent** **AF-14**	The solution shall enable the Map Extents boundaries to be configurable by an authorised user.	Must
Configure **control centre** **AF-15**	The solution shall enable additional control centres to be configured. Please outline the role and responsibilities of TfL and the Service Provider where TfL require the implementation of an additional control centre.	Must

Transport for London

Ref	Description of Requirement	Priority
4.15. Migration of existing incident data The solution implemented will require to hold data on incident migrated from the existing platforms currently used within TfL. The data migration will include historic incidents and possibly also ongoing incidents, depending on the cut-over. The following section outlines the responsibility for each step of data migration. The solution will not extract Incident and Diversion data for TfL existing applications, this will be managed by TfL.		
Transform rules **MR-01**	The Service Provider shall provide a transformation specification, post award, to enable TfL data to be migrated to the solution.	Must
Load mechanism **MR-02**	The Service Provider shall provide a mechanism to load existing TFL incidents into the solution	Must
ETL analysis **MR-03**	The Service Provider shall provide error analysis and exception reporting of the transform and load of TfL incident data.	Must
Data storage – migration volume **MR-04**	The solution shall support initial data migration transaction volumes of 7 years of transactions;(see document ref 1) approx 70,000 incidents for LUCC, and for CentreComm approx 2.5 million incidents for previous 7 years.	Must
Existing data **MR-05**	The solution shall provide a means of storing and accessing existing incident data in a read-only format, until deleted in line with the data retention schedule document ref 1. The data retention period is as defined in Ref 1 for CentreComm and LUCC data	Must

Transport for London

5. Non-Functional Requirements

Unless otherwise stated, please confirm your approval and where appropriate provide a detailed response of how you would conform to the requirements listed below, using a maximum of 200 words for each response unless otherwise indicated (in some instances, if more words are required, please indicate a valid reason)

Requirements are prioritised using the MoSCoW method:

- **M** – MUST: Describes a requirement that must be satisfied for the solution to be considered a success.

- **S** – SHOULD: Represents a high-priority item that should be included in the solution if it is possible. This is often a critical requirement but one which can be satisfied in other ways if strictly necessary.

- **C** – COULD: Describes a requirement which is considered desirable but not necessary. This will be included if time and resources permit.

- **W** – WON'T: Represents a requirement that stakeholders have agreed will not be implemented in a given release, but may be considered for the future.

Ref	Description of Requirement	Priority

5.1. Features: Shared Platform

The business processes operated by LUCC and CentreComm are separate and distinct therefore the solution must reflect this. Due to the nature of the respective operating environments, it cannot be assumed that pan-TfL business processes will be devised to accommodate the new solution.

Multiple presentations SP-01	The solution shall enable multiple presentations to different control centres.	Must
Separation of data **SP-02**	The solution shall be secured appropriately to respect organisational boundaries, i.e. by default there must be no visibility of incident data between the two business areas.	Must

Transport for London

Ref	Description of Requirement	Priority
Operational viewpoint **SP-03**	The solution shall not be optimised for one business area at the expense of the other, e.g. there must be no visibility of CentreComm specific drop down values and fields in LU or vice-versa.	Must
Sharing by exception **SP-04**	The solution shall enable data sharing for exceptional circumstances, such as major incidents or events that affect multiple locations across London.	Must

5.2. Features: Interfaces

Please demonstrate how your solution will achieve the objectives below – please see figure 1 above - max of 2000 words

Req Title	Requirement Description	Priority
CentreComm Incidents to CDR **IF-01**	The solution shall enable an interface to the TfL Central Data Repository (CDR) for new and updated Incidents via open interface standards; see section 7 for data field description. Note: Control Centre Desk Logs are not sent to CDR. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
CentreComm Incidents to CDR **IF-02**	The solution shall shall enable Incidents to be fed through to the CDR at least every ten (10) minutes via open interface standards. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

Transport for London

Req Title	Requirement Description	Priority
CentreComm Diversions to CDR IF-03	The solution must enable an interface to the CDR for new and updated Diversions via open interface standards see section 7 for data field description. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
CentreComm Diversions to CDR IF-04	The solution shall enable diversions to be fed through to the CDR at least every ten (10) minutes via open interface standards. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must
TfL Reference Data as a data source IF-05	The solution shall enable dynamic access to TfL-maintained reference data in the CDR via open interface standards (e.g. Bus Reference Data; Bus Routes, Stops, Turning Points etc) – listed in Section 7.	Must
"ESRI as a Service" as a data source IF-06	The solution shall enable dynamic access to TfL-maintained reference data in TfL's ESRI as a Service via open interface standards (e.g. Bus Reference Data; Bus Routes, Stops, Turning Points etc) – listed in Section 7. Note: "ESRI as a Service" is based on an ESRI Server which holds GIS and mapping data for a number of TfL's Traffic systems, using the ITN and TOIDS. **This requirement may not be implemented on initial go-live.**	Must
XIS as a data source IF-07	The solution shall enable dynamic access to TfL-maintained reference data via the TfL Enterprise Data Bus, XIS, via open interface standards (e.g. Bus Reference Data; Bus Routes, Stops, Turning Points etc) – listed in Section 7. **This requirement may not be implemented on initial go-live.**	Must

Transport for London

Req Title	Requirement Description	Priority
External Reference Data **IF-08**	The solution shall enable dynamic access to 3rd party supplied reference data via open interface standards – listed in Section 7.	Must
Mobile location **IF-09**	The solution shall interface with TfL's current mobile phone provider (O2) to locate the position of the Duty associated with the mobile via open interface standards.	Must
External Bulletin Board **IF-10**	The solution shall interface with an external facing bulletin board (this is currently provided via Google Blog) via open interface standards.	Must
SMS/ email service **IF-11**	The solution shall interface with TfL's messaging service provider (currently PageOne) via SMS integration using SOAP/ XML protocol, see Ref 11.	Must
Cognito PDA handheld **IF-12**	The solution shall interface with the Cognito PDA solution to receive logon/logoff and available/not-available transactions from Resources via open interface standards.	Could
SharePoint (NOE) **IF-13**	The solution shall interface with the TfL Notice Of Event SharePoint site via open interface standards.	Should

Transport for London

Req Title	Requirement Description	Priority
Business intelligence tool **IF-14**	The solution shall interface with a TfL business intelligence tool via open interface standards	Must
iBus **IF-15**	The solution won't interface with iBus for bus location via open interface standards. The call details from iBus (or its equivalent) will include but not be limited to; • Route no • Running No • Bonnet Number • Location (x/y co-ordinates) • Direction of travel.	Won't
Traffic circulars **IF-16**	The solution won't interface with the Traffic Circulars via open interface standards. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Won't
Masternaut **IF-17**	The solution won't interface with Masternaut for LU Emergency Response Units' location via open interface standards. For the avoidance of doubt this requirement shall not apply to the CentreComm DC.	Won't

"A high level view of interfaces required can be seen on Figure 1, Scope of project for Control Centres systems in Section 2.3

Transport for London

Req Title	Requirement Description	Priority
5.3. Features: Adaptability, Future-proofing and Design		
Backward compatibility **FP-01**	The solution shall provide a roadmap to support access to data from legacy versions as a solution develops over time.	Must
Integration with industry standard APIs **FP-02**	The Service Provider shall list all APIs to support system extensibility, data exchange and integration capability in line with industry open standards.	Must
Integrate TfL's "ESRI as a Service" **FP-03**	The solution should enable use of TfL's ESRI as a Service via open interface standards. The solution should be able to be re-configured to utilise this service as an alternative to the supplier-provided solution. Note: "ESRI as a Service" is based on an ESRI Server which holds GIS and mapping data for a number of TfL's Traffic systems, using the ITN and TOIDS. FYI: TfL's end user licensing for the ESRI GIS data product will cover development use by third parties. It will allow access to the ESRI developer network. **This requirement will not be implemented on initial go-live.**	Should
Code ownership **FP-04**	All configuration and customisations developed for this COTS solution shall be owned outright by TfL and all code will be developed, documented and commented according to industry standards (TfL may provide an independent tester to confirm this).	Must

Transport for London

Req Title	Requirement Description	Priority
5.4. Features: Accessibility and Usability		
Content accessibility guidelines **AU-01**	Where relevant, the solution shall be built to uphold level 'AA' of the WAI's Web Content Accessibility Guidelines (WCAG 1.0) as a minimum standard.	Must
Data access **AU-02**	The solution shall ensure access, extraction and export of TfL data using non-proprietary industry standard tools, following expiry of the contract.	Must
5.5. Features: Connectivity		
Desk top Futures **CN-01**	The solution shall support the TfL OneLondon Windows 7 / IE9 / Windows Server 2008R2 based Desktop Futures environment, including access via Citrix-based T-SNAP remote desktop sessions.	Must
Web browser neutral **CN-02**	Where the solution access is via a web browser, the client access must be web browser agnostic. Note Windows 7 SP1, IE 9 and above, Windows XP SP3 IE 7 and above may still be on the TfL estate.	Must
Access devices **CN-03**	The solution shall provide access via a mobile device to a limited set of functionality	Could

Transport for London

Req Title	Requirement Description	Priority

TfL enterprise platforms
 	
CN-05
	An internally hosted solution shall be deployable on the operational versions of the following major technologies as deployed within the TfL estate, see also ref 5;
	
	  a) MS Windows Server 2008 R2 / 2012
	
	  b) Solaris 10 update 11, Red Hat Linux 6.5
	
	  c) VMWare 5.1
	
	  d) Citrix XenDesktop / XenApp V6.5 and Appsense V8
	
	  e) SQL 2008R2 / 2012 Always On,
	
	  f) Oracle 11g R2 RAC
	
	  g) Windows 7 SP1, IE 9 and above, Windows XP SP3 IE 7 and above may still be on the TfL estate,
	
	  h) ODBC / JDBC drivers' connectivity,
	
	  i) Industry standard Web services / XML and messaging protocols,
	
	  j) Integration with the Enterprise Service Bus, specifically TIBCO products.
	
	  k) Both Block and CIFS storage is available.
		Must

TfL enterprise platforms **CN-06**	Regarding interfacing with a proposed Enterprise Service Bus, how will your solution integrate with JMS (Java Message Service), industry standard Web services / XML and messaging protocols for Enterprise Service Bus integration (e.g. TIBCO products)?	Must

Transport for London

Req Title	Requirement Description	Priority
TfL enterprise platforms **CN-07**	The supplier shall describe the standards and technologies followed in delivering the solution interfaces (e.g. SOA, etc.)	Must
TfL enterprise platforms **CN-08**	At TfL's discretion, the supplier shall undergo phased approach with the implementation of interfaces with sequential deployment, testing and sign-off before continuing. .	Must

Req Title	Requirement Description	Priority
5.6. Security and Compliance: User Identification, Authentication and Authorisation The solution must provide authorised Admin users with the facility to grant valid One London users access to the solution – initial access must be controlled by One London Active Directory authentication		
AD for authen **AA-01**	The solution shall be compatible with TfL's current authentication and authorisation method; currently Active Directory.	Must
Single signon **AA-02**	The solution shall enable single signon, via Active Directory.	Should

Transport for London

Req Title	Requirement Description	Priority
User Accounts **AA-03**	The solution shall allow an administrator function to map to the Active Directory account for each user at a system-wide level.	Must
Variable Access Levels **AA-04**	The solution shall allow an administrator to grant individual users and groups variable user privileges.	Must
Role-based Access **AA-05**	The solution shall provide for user privileges to be assigned according to user roles, see Section 3.2, Role Types.	Must
Admin Accounts **AA-06**	The solution shall provide for the creation of administrative user accounts for a business area.	Must
User Groups **AA-07**	The solution shall enable the system administrator to manage (i.e. create, amend and delete) user groups.	Must
User groups features **AA-08**	The solution shall provide a flexible application security model that enables the system administrator to enable/disable particular features for specific users groups.	Must

Transport for London

Req Title	Requirement Description	Priority
User access types **AA-09**	The solution shall be able to be deployed to different environments depending on role and access required; • OneLondon desk top / back office environment for Operators, Admin, functionality governed by Role, • Limited functionality access (could be via a mobile platform) for Weather readiness reporting, • Read only access to information dependent on role (possibly via a mobile platform), • Communication recipients, (no solution access required) • Emergency alert recipients (these may be identified by i/p address), no signon access required.	Must

Req Title	Requirement Description	Priority
5.7. Security and Compliance: Auditing		
Track Changes **AT-01**	The solution shall maintain an audit trail of all changes made to data.	Must
Track Attachment Changes **AT-02**	The solution shall maintain an audit trail of all the changes to the attachments. (The audit trail is not required to track internal changes to the attachments themselves, but only to record the fact that attachments have been added, replaced or removed.)	Must

Transport for London

Req Title	Requirement Description	Priority
Track activity **AT-03**	The solution shall maintain an audit trail of all user sessions (i.e. session start, duration and finish, privilege allocations, amendments, and elevations).	Must
View Tracked Changes **AT-03**	The solution shall allow users to view the audit trail of tracked changes that is held.	Must
Audit log integrity **AT-04**	The solution shall ensure that the integrity of audit logs is protected from any editing or deletion.	Must
Audit viewing **AT-05**	The solution shall maintain an audit trail of all the opened or viewed incidents and events performed by a user.	Must
5.8. Security and Compliance: Regulatory and Legal Compliance The requirements specifically related to the application's need to be legal and compliant with relevant legislation. Note, the solution does not have any CPNI regulatory framework requirements.		
DPA compliance **LC-01**	The solution shall enable compliance with the Data Protection Act. Personal data may occasionally be captured by the Control Centre in the process of managing an incident that could identify an injured party.	Must

Transport for London

Req Title	Requirement Description	Priority
Privacy and data protection risks **LC-02**	The Service Provider must be able to proactively identify privacy and data protection risks/issues and describe the types of scenario that would constitute a breach of policy and/or the law. They should have systems in place to identify, monitor and resolve security incidents involving personal data.	Must
Responding to SAR **LC-03**	The Service Provider must be able demonstrate how to respond to Subject Access Requests (SARs) for personal data made under relevant privacy and data protection legislation with an understanding of what these involve and how these may impact the Service Provider. To include a description of the Service Provider's information and document management processes that would support retrieval of personal information if requested by a Data Subject.	Must
Data privacy training **LC-04**	The Service Provider shall demonstrate how: training employees and temporary workers on privacy and data protection issues, and monitoring of workforce compliance with privacy and data protection requirements are completed. The Service Provider shall be able to demonstrate that all employees and temporary workers (including contractors and consultants) with access to personal information, are appropriately trained (including high level specialist training where necessary) and that refresher/update training is provided periodically.	Must
Data privacy audits **LC-05**	The Service Provider sjhall show that audit/assurance arrangements are in place to monitor compliance with relevant legal and best practice requirements; and are used to deliver improvements with specific regard to privacy and data protection compliance.	Must

Transport for London

Req Title	Requirement Description	Priority
5.9. Security and Compliance: Data Integrity and Privacy		
Back up DP-01	The solution shall be able to support compliance with TfL data backup standards. The Retention policy, see Ref 1 defines how long the data that is backed up remains valid for and therefore how long it should be stored.	Must

Back up Type	Retained for
Keep dailies for:	31 days
Keep weeklies for:	4 weeks
Keep monthlies for:	84 months
Keep yearlies for:	7 years

Req Title	Requirement Description	Priority
Retention period **DP-02**	The solution shall enable the retention period requirements to be implemented, see document ref 1.	Must

Transport for London

Req Title	Requirement Description	Priority

Data security classification
 	
DP-03
	The solution shall enable the information classification standard requirements to be implemented as follows; See document ref 2;
	
	    o Incident data will fall under the remit of the Data Protection Act as personal data could be recorded about individuals involved in an incident, so TfL_RESTRICTED Part 2,
	
	    o Contingency Plans recorded by LUCC is in the TfL-Confidential category,
	
	    o Information sent out via the broadcast messages and alerts will be TfL_RESTRICTED Part 1.
		Must

5.10.   Security and Compliance: Security Requirements

Req title	Requirement Description	Priority
Software development **SR-01**	The organisation engaged to develop the solution shall ensure that all software and systems are developed and maintained in a secure manner in line with TfL's software development security policy, see document ref 4.	Must
Information Security Control Framework **SR-02**	The Service Provider shall demonstrate compliance, with evidence provided, with all the security controls in the TfL Information Security Control Framework, see document ref 12. The Service Provider must complete Ref 6	Must

Transport for London

Req title	Requirement Description	Priority
Service Provider **security** **SR-03**	The Service Provider shall provide information regarding the security aspects of their proposed solution. The Service Provider shall demonstrate that any information stored on its systems that relate to this contract or the operation of this contract be protected by all reasonable means. Information that needs to be protected includes, but is not limited to: o Staff data, such as names, account names, e-mail addresses, locations and phone numbers o Details relating to technical specifications or configurations used within the TfL estate, including the network o Passwords and encryption keys o Commercial arrangements	Must

Req Title	Requirement Description	Priority
5.11.	**Delivery: User Documentation and Help**	
Contextual help **DH-01**	The solution shall provide an Online help facility with contextual help depending on the user location.	Must
Error messages **DH-02**	The solution shall provide meaningful error messages to users when faced with invalid user input; however sufficient fault diagnosis and logging must not be compromised.	Must
User FAQ **DH-03**	The solution shall make an FAQ (Frequently Asked Questions) list for the most Common Error Message to be available for users.	Should

Transport for London

5.12. Delivery: Design process

Req title	Requirement Description	Priority
Project management methodology **PR-01**	The Servoice Provider shall describe its Project Management methodology and lifecycle, and specifically state how it will be applied to ensure the successful delivery of the MICCS requirements. The response must include clear descriptions of the Project Management techniques and tools that will be used (for example Risk Management). The response should also include a description of how the following stages will be delivered and managed including a description of key deliverables of each stage: 1. Requirements Validation 2. Functional Specification 3. System Design 4. System Configuration and Development 5. System Testing & Acceptance 6. Training Dependencies on TfL shall be clearly specified in the response. The Service Provider should be aware that TfL will manage the project in accordance with their version of the PRINCE2 methodology. The Service Provider s should allow for PRINCE 2 Gate approval processes to be completed at appropriate milestones in the delivery.	Must

Transport for London

Req title	Requirement Description	Priority
Team structure **PR-02**	The Service Provider shall describe the project team structure that will be used. The roles, delivery locations and organisations must be specified. Clear lines of accountability must be shown - including contractual relationships where work is subcontracted. Where work is sub-contracted, the Service Provider shall describe how this work will be managed to ensure delivery to time, cost and quality requirements. Interfaces to TfL must be clearly identified and communication methods described.	Must
Iterative design **PR-03**	The Serviuce Provider shallensure that a reasonable iterative design process can be undertaken for all aspects of the project.	Must
Human factors **PR-04**	The Service Provider shall ensure that the design of the user interface shall place Human Factors as the highest priority in delivering the required functionality.	Must
ISO standards **PR-05**	The Service Provider shall ensure that the design demonstrates adherence to ISO 11064 2006 or other relevant standards	Must
User interfaces **PR-06**	The Service Provider shall build interactive mock User Interfaces during the design process to gauge the Users' perception, and to validate the User Interfaces' "look and feel".	Must

Transport for London

Req title	Requirement Description	Priority
Migration design **PR-07**	The Service Provider shall ensure that the solution is designed such that during Migration there is no impact on operations due to conflicts between the legacy and new solution.	Must
User interface and equality Act PR-08	The Service Provider shall follow best practice guidance in the design of the User Interface, including requirements to meet Equality Act 2010.	Must
Development and Support **PR-09**	TfL will provide the underlying environments required to enable solution development, including but not limited to development, test, pre-production environments, etc, and may make these environments available to the winning supplier via remote access. The intention is to provide a facility where the supplier can develop and deploy to ensure a fully working solution is delivered and remove the risk of deployment issues emerging. Post implementation, TfL's intention is to provide remote access to the TfL environment, appropriately controlled, for the supplier to remote in with priviledged access as required. The Service Provider is asked to confirm acceptance of this requirement and comment on whether all development and testing can be on a TfL environment.	Must

5.13. Delivery: Installability/ Deployment approach

Req title	Requirement Description	Priority

Transport for London

Req title	Requirement Description	Priority
Virtualisation **DA-02**	The solution shall be compatible with TfLInfrastructure requirements, see ref 5.	Must

Req Title	Requirement Description	Priority
5.14. Service Related: Availability and Recoverability The project currently has 2 measures aimed at restoring a full service after Primary site failure: • RPO (Recovery Point Objective) – maximum data loss period • RTO (Recovery Time Objective) – maximum time to bring back the service Control centre-specific RTO and RPO were originally specified to illustrate the slightly different nature of the call behaviour. TfL do not expect a solution to be implemented with varying RPO and RTO. Both control centres will align to the requirements of the more demanding RPO/RTO. LUC will align with the CentreComm RPO / RTO requirements so the LUCC specific RPO/RTO requirements have been removed.		
Core hours support required **AR-01**	The solution will require support during 24 /7 operation 365 (366) days of the year.	Must
99.88 % availability **AR-02**	The solution shall be designed and implemented to be available 99.88% of the time, measured annually, excluding agreed scheduled downtime. Therefore, the unplanned system downtime must not exceed 10.5 hours in any calendar year.	Must

Transport for London

Req Title	Requirement Description	Priority
Application level failover AR-03	The solution shall be designed to implement active / active standby in a secondary data centre to enable application level failover.	Must
Recovery Time Objective (RTO) AR-04	In the event of a disaster (i.e. a complete failure of a data centre) being declared in the primary site the solution shall be recoverable in the secondary site within 1 hour, i.e. have a Recovery Time Objective (RTO) **of 1 hour**.	Must
Recovery Point Objective (RPO) AR-05	In the event of a disaster (i.e. a complete failure of a data centre) being declared in the primary site the Recovery Point Objective is 30 **seconds** (RPO).	Must
High Availability AR-06	The solution as deployed in the Primary Site shall not have a single point of failure in its infrastructure, with any single interruption in service limited to **30 minutes**.	Must
Local availability AR-07	The solution could enable local working in the event of a back end or Data centre failure, enabling users to continue to work locally during a failure and then commit information when full functionality is restored. This may be delivered via a thick–client implementation, for example. Please provide a reference architecture and description for your proposed solution, demonstrating how your solution will achieve this objective –	Could

Transport for London

Req Title	Requirement Description	Priority
Recover to consistent state **AR-08**	Should the solution or any component of it fail and subsequently need to be restored, the state of the solution, its functionality and all data within shall be restored to a consistent state. (i.e. without the need for manual data changes to ensure that records in one data structure are reflected in others).	Must
System status **AR-09**	The state of the solution upon restore shall be discernible by Transport for London and London Underground at the time at which the solution is restored. e.g. if 10 minutes of data has been lost, Transport for London must be able to easily determine that fact without having to search for changes made or data entered that may have been lost.	Must

5.15. Service Related: Transaction Volumes

Req title	Requirement Description	Priority
Data storage – changes **TV-01**	The solution shall ensure there is no impact on performance from other systems running on the same platform.	Must

5.15.1. Transaction volume – LUCC specific requirements

Current LUCC Incidents 100 incidents / day, approx 10 affecting service, with an average of 10 actions (i.e. transactions) for an incident. Some incidents will generate several hundred transactions.

Data growth: It is anticipated that the volume of data will grow in the coming years, assume 10% growth.

Transport for London

The design of the solution must be able to accommodate changes in terms of capacity and performance

Req title	Requirement Description	Priority
Data storage – changes TV-02	The solution shall support an average daily transaction volume changes between 1,000 and 2,000, either modifications to existing incidents or new incidents being added. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Transaction types **TV-03**	There are no specific patterns of incident types requiring to be demonstrated. Demands on the service will vary depending on peak travel times and one –off events. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	For info in testing
Activity pattern **TV-04**	There is no specific pattern of incident over the day / week requiring support. Peak usage will vary across the week and year with season, events and other external factors. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	For info in testing

5.15.2. Transaction volume – CentreComm specific requirements

The assumption is that incident each will be re-opened an average of once to update and/or Clear.

Req title	Requirement Description	Priority

Transport for London

Req title	Requirement Description	Priority
Data storage – changes **TV-05**	The solution shall support the following expected volume of activity without impacting the response times: • 700-1000 New Incidents / Day, generating approx 2,000 transactions / day. • 500 Other transactions / Day including new Diversions, Ticket Requests, Control Centre Logs and Events • A minimum of 10 Scheduled Reports run each day • 100 Resource log on/off transactions each shift change (currently at 0600, 1300 and 1800 each day). • Polling the location of a minimum of 40 logged on Resources every 10 minutes, over a 24 hour day. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must

5.16. Service Related: Capacity

Req title	Requirement Description	Priority
Capacity **CP-01**	The solution shall support the following user capacity profile.	Must

The number of users of the solution has the potential to increase. As of June 2013, the table below represents the estimated number of users. The type of support user or user users required will depend on the solution implemented.

Transport for London

User Type	Number of current users	Number of potential Users	Number of Concurrent Users
Current			
LUCC Operators	70	70	15
Read only LUCC	140	200	100
CentreComm operators	200	200	25
Communication recipients	40 Garages 4,000 users	Not known	Not known
Weather readiness reporters	100	200	15
Alert Recipients	9	9	9

Req title	Requirement Description	Priority
Future user capacity **CP-02**	The solution shall have the ability to accommodate the following additional users without re-design of the solution.	Must

User Type	Number of current users	Number of potential Users	Number of Concurrent Users
Power control room	0	60	Potentially 20
Line Control Centres	0	700	Potentially 100
Station staff	0	3000	Potentially 500
Surface control centres	0	100	25

Transport for London

- CentreComm Operators working in 12 hour shifts (24hrs / Day)

- Typical usage per CentreComm shift is approx 12 – 17 concurrent users

Req Title	Requirement Description	Priority
User Volumes – concurrent **CP-03**	The solution shall support: •Minimum of **25 CentreComm** concurrent users, with capacity for rise to **100 CentreComm** concurrent users, •Minimum of **15 LUCC** concurrent users, with capacity for rise to **50 LUCC** concurrent users, This future-proofs the solution for expansion.	Must
User Volumes – total **CP-04**	The solution shall support: •Minimum of **200 CentreComm** registered user accounts, and a maximum of **1,600** users, •Minimum of **300 LUCC** registered user accounts, and a maximum of **5,000** users.	Must

5.17. Service Related: Response Times

The following Solution response times are critical for usability in any control centre. Calls can be as short as 20-30 seconds during which time all pertinent details must be captured by the User in the solution.

Req title	Requirement Description	Priority

Transport for London

Req title	Requirement Description	Priority
Sub-second data entry RT-01	The solution shall support sub-second response times for user input on forms-mode interactions There shall be no discernible keystroke delays during field or text entry.	Must
Long running task progress RT-02	The solution shall provide progress and an accurate estimate to complete on any long-running task.	Must
Performance RT-03	The following performance requirements shall be achieved for a user, regardless of load: a. **Incident Queue Screen Refresh:** The Incident Queue screen must refresh within 0.5 seconds and display any new Incidents or records that have been created or updated by other Users. b. **Forms:** Data entry forms must be presented on screen within 0.5 seconds of the User selecting the function via a menu / button or via a Short Key. c. **Save:** Data on all forms must be saved and the user returned to the main screen within 0.5 seconds of a Save operation being selected. d. **Record Retrieval:** When a record (e.g. an Incident) is selected from the Incident Queue screen, the data must be presented within 1 second. e. **List Retrieval:** When retrieving a list of Open Incidents (e.g. to assign a Resource) the list must be presented within 2 seconds. f. When a new Incident is created, **candidate lists** (for duplicates or previous calls) must be displayed within 2 seconds of matching data fields being entered.	Must

Transport for London

Req title	Requirement Description	Priority
Performance mapping RT-04	**a. Map / Street Search:** Street searches shall be retrieved and presented on the map screen within 1 second, including layered data. **b. Map Pan and Zoom:** Map screens shall be displayed without noticeable delay (no tiling effect or staggered presentation) when the user pans the map screen or zooms in/out. Either by mouse dragging, clicking or zooming in/out with on screen control tools. **c. Icon Data Retrieval:** Data associated with Map Icons (e.g. Resources, Bus Stops, CCTV cameras) shall be displayed within 1 second. For the avoidance of doubt this requirement shall apply to both LUCC and CentreComm	Must
Performance – CentreComm specific RT-05	a. **Assignment:** When assigning a Diversion or Resource to an Incident, the assignment shall be completed within 1 second. b. **Bus Route street data** shall be retrieved within 0.5 seconds of the Bus Route being entered by the User in an Incident form. For the avoidance of doubt this requirement shall not apply to the LUCC DC.	Must

5.18. Service Related: Support and Maintenance

Req title	Requirement Description	Priority
Monitor system availability SM-01	The solution as a whole shall be monitored such that its true availability can be assessed at any point in time by Transport for London.	Must

Transport for London

Req title	Requirement Description	Priority
Integrate with SCOM and Ionixs **SM-06**	The Service Provider must make all relevant data available to SCOM (System Center Operations Manager / OpsMgr 2012) and IONIX.	Must
SCOM management pack **SM-07**	The Service Provider could provide a SCOM management pack for their solution. Please demonstrate if and how your solution achieves this objective	Could
SCOM management pack SM-08	Following on from SM-07, if a SCOM management pack is not available, The Service Provider shall allow TfL input into its definition of a custom SCOM management pack.	Must
Service reporting capability **SM-09**	The solution shall provide a comprehensive set of reports on the service performance and availability.	Must
Monitor system performance **SM-10**	All components of the solution, including all interfaces, servers, batch processes and integration points shall be monitored for performance and the solution as a whole must be monitored using event correlation such that its performance health can be assessed at any point in time by Transport for London.	Must

Transport for London

Req title	Requirement Description	Priority
Service support **SM-11**	The service centre functions that support the solution, where provided by the Service Provider, shall be correlated with the service centre functions undertaken by Transport for London such that call handovers, regardless of the level of support, can be performed with limited to no impact upon users of the solution (e.g. users should be able to seek an update on a fault that was raised with one party from another party by providing the original call logging number). In order to deliver the RPO & RTO specified, 24 / 7 support is required.	Must
Schedule jobs **SM-12**	The solution shall support the ability to schedule functions within it such as system maintenance activities, long running jobs or the generation of reports.	Must

5.19.   Service Related: Service Management requirements

Req Title	Requirement Description	Priority

Transport for London

Req Title	Requirement Description	Priority
Patching **SA-02**	TfL need to ensure that our live operational services are correctly patched and updated to ensure that systems are current and supportable. This applies to allow components of services, including hardware, operating system, and software. The Service Provider is asked to provide a schedule of planned patches and updates to their current solution over the next 12-15 months.The Service Provider shall define their patching and update process and how they will involve TfL in that process. The Service Provider shall outline their approach to ensuring that the system continues to work with updates and patches to the operating system being implemented by TfL, outline the testing that they believe will be required, and confirm what they require of TfL in order for the Service Provider to fulfil this requirement, The Service Provider shall confirm that all patches, updates and associated testingwill be provided at no additional charge throughout the term of the agreement. See also ref 3	Must
Roadmap **SA-04**	The Service Provider shall provide product roadmaps for all software products required in the delivery of the service, including upgrades, end of production and end of support dates, as well as suggest replacement products where applicable. How does the Service Provider propose to communicate this to TfL during the life of this agreement? Updated roadmaps are required a minimum of annually. The Service Provider is to confirm the frequency of their updates. .	Must

Transport for London

Req Title	Requirement Description	Priority
Software support - Adherence to TfL Policies **SA-05**	TfL strictly tests and approved all new software (including version upgrades) that come on to its estate for compatibility with our existing infrastructure. How would the the Service Provider ensure that this policy is adhered to and that only approved software is deployed? The Service Provider's response should include, but not be limited to: End to end process, Tools, Frequency, and Scheduling.	Must
Warranty **SA-06**	The Service Provider shall asked to confirm periods of warranty. What levels of support are provided during this period? The Service Provider shall confirm that this warranty period is provided at no additional cost to TfL.	Must
Maintenance **SA-07**	How would the Service Provider ensure that all source code, data, documentation and any other key information required by TfL in a force majeure situation is accessible? The Service Provider shall detail processes and tools in place to safeguard TfL data and security. The Service Provider's response should include, but not be limited to: tools, processes, success factors, any industry standard safeguards.	Must
Licence Management **SA-08**	The Service Provider shall ensure that all software licence documentation and physical media are sent to TfL's Licence Management Team. The Service Provider shall detail any processes, procedures and software tools used to control software, software/code versions and releases. The Service Provider shall detail how they would manage software asset, does the Service Provider have their own licence management functions. Does the Service Provider carry our regular audit of software assets? Can the Service Provider provide comprehensive logs of all software assets? TfL operate an environment of both traditional thick client desktops and thin clients. The Service Provider are to ensure that their proposed solution is compatible with the contained technical outline of TfL operating environment ensuring availability on both 'thick' and 'thin' clients'.	Must

5.20.   Service Related: Service Operations requirements

Req Title	Requirement Description	Priority

Transport for London

Req Title	Requirement Description	Priority

Service Desk – Arqiva's **own Service Desk** **SO-01**	The Service Provider shall provide details on their Service Desk function, including:
	   o Roles and Responsibilities.
	   o Number of full time equivalents providing support.
	   o Service Levels including, but not limited to, call handling response times, and call abandonment rate and management of escalations.
	   o Hours of Operation
		Must

Service Desk – interface with TfL IM Service Desk **SO-02**	TfL have a preference for TfL end user incidents and requests to be handled by TfL's Service Desk Provider and for TfL's Service Desk Provider to be the single point of contact for The Service Provider.
	
	 TfL have a preference for the Service Desk Provider's primary interface with the Service Provider to be via telephone.
	
	 The Service Provider shall describe their proposed mechanism(s) that will be deployed to exchange information with TfL's Service Desk Provider and other TfL service providers, covering areas such as:
	
	   o The exchange and status of information for incidents, requests, changes and releases.
	   o How the two organisations will cooperate to identify the causes of any faults, particularly where it is not immediately clear on which side of the service boundary the fault lies.
		Must

Service Desk **SO-03**	How will Arqivathe Service Provider ensure that TfL's Service Desk can resolve as many Incidents on a first time fix basis as possible?	Must
Change Management **SO-04**	The Service Provider shall align with the TfL Change Management process, see document ref 8. The Service Provider is to confirm acceptance of this requirement or propose alternative approaches. The Service Provider is requested to describe their approach to Change Management and any toolsets used with respect to the operational change management process.	Must

Transport for London

Req Title	Requirement Description	Priority
Release Management **SO-05**	The Service Provider is required to align with the TfL IM Release Management standard, see document ref 9. • The Service Provideris asked to confirm acceptance of this requirement • The Service Provider to respond specifically to each section of the IM Release Management standard • The Service Provider to clarify how their processes meet the standards specified • Any areas where the standard cannot be met or any other exceptions must be detailed with reasons and alternatives The Service Provider shall take part in discussions to have release and deployment processes agreed and documented within the service's Support Model, and is asked to confirm acceptance of this requirement	Must
Incident Management – SLAs **SO-06**	The Service Levels for incident restore, work around or agreed plan to restore are contained in the Service Level Agreements as described in section 5.20.1 TfL Service Level Agreements. The Service Provider shall confirm acceptance and adherence to these requirements or propose achievable service level targets.	Must

Incident Management
 	
SO-07
	The Service Provider shall describe their proposed Incident Management process to ensure that users receive an end to end service, including items such as:
	   o Event detection, recording and classification.
	   o Investigation and diagnosis.
	   o Reporting and status updates.
	   o Resolution and recovery.
	   o Incident closure.
	   o Liaison with third parties.
	
	   o Major incidents.
		Must

Transport for London

Req Title	Requirement Description	Priority
Incident Management **SO-08**	The Service Provider shall describe their system and application event monitoring and alerting, and how such alerts are handled.	Must
Problem Management **SO-09**	The Service Provider shall describe their Problem Management process and approach to: o Identification, investigation and diagnostics. o Proactive trend and cause analysis. o How known errors will be handled and the resolution or workaround communicated. o Reporting and status updates.	Must
Problem Management **SO-10**	The Service Provider shall undertake trend and cause analysis and problem reviews in order to assist in the resolution of incidents and to prevent recurrence of incidents. The Service Provider s shall describe: o How such reviews would be initiated (i.e. trigger events and performance targets). o How such reviews would be conducted.	Must
Problem Management **SO-11**	The Service Provider shall work with TfL's internal resolver groups and other third party vendors in order to resolve incidents (including security) that fall under their joint responsibility. The Service Provider shall describe their approach to the following: • How the service on both sides of the interface will be monitored, including the exchange of status information; • How the organisations will cooperate to identify the causes of any faults/incidents, particularly where it is not immediately clear on which side of the service boundary the fault/incident lies; • Escalation processes to ensure that the appropriate technical resources are available and applied to rectifying service issues.	Must
Minor changes of a pre-agreed type **SO-12**	The Service Provider shall enter into discussion on SLAs to be agreed for Request Response and Resolution Times for minor changes of a pre-agreed type in line with business requirements The Service Provider shall confirm acceptance and adherence to these requirements or propose achievable service level targets.	Must

Transport for London

Req Title	Requirement Description	Priority
Capacity Management **SO-13**	The Service Provider shall outline how they would measure capacity for the service and the infrastructure required to deliver it? The Service Provider are asked to outline how they would manage a lack of capacity? • What is the Service Provider's approach to collecting, managing and presenting capacity and availability data? • How will peaks and troughs and other anomalies be shown as part of capacity and availability reporting? • Please provide sample capacity management reports.	Must
Availability Management **SO-14**	The availability target will be aligned to requirements detailed within the Non Functional Requirements (see section 5.14 Availability and Recoverability). The service must not be impacted by any systems maintenance or management activities such as software or hardware upgrades without prior agreement with TfL. The Service Providershall detail planned maintenance windows and shall ensure that all maintenance windows are agreed with TfL in advance. If necessary, maintenance will be done outside of the core hours without any additional costs incurred. The successful Service Provider will take part in discussions to have these agreed and documented within a Service Support Model. The Service Provider is to confirm acceptance of these requirements or propose alternative approaches.	Must

Transport for London

Req Title	Requirement Description	Priority

Configuration Management
 	
SO-15
	TfL seeks to maintain an accurate CMDB (Configuration Management Database) which contains details of all CIs of the end-to-end service.
	
	This requirement applies to CIs (Configuration Items) which are the responsibility of The Service Provider . The Service Provider shall describe their approach to Asset and Configuration Management paying particular attention to how asset and configuration item (CI) information will be updated and maintained.
	
	The Service Providershall be responsible for the timely update of the TfL CMDB for all TfL assets under the Service Provider's responsibility. To achieve this, they will be required to submit to TfL information on the CIs which are their responsibility, using the template that will be provided by TfL, to allow update of TfL IM's CMDB. This includes all installations, moves, changes and decommissions that involve TfL owned assets, regardless of what triggers the action.
	
	The Service Provider shall maintain a register of all assets required in the provision of the service, including but not limited to:
	  o Asset type and model, version
	  o Specification (including peripherals)
	  o Platform
	  o Location
	  o Support arrangements
	  o Date of install (where installed by The Service Provider)
		Must

Service /Business Continuity
 	
SO-16
	The Service Provider shall describe fully the IT Service Continuity Management (ITSCM) considerations for providing this service/s including how they would envisage recovery (including timescales) of the system/s following a disaster, including such items as:
	  o Disaster recovery invocation
	  o Live running during disaster recovery period
	  o Reversion to normal operations at the end of the disaster recovery period
	  o Disaster recovery tests (including frequency)
	  o Business continuity plans
	  o Impact to TfL
		Must

Transport for London

Req Title	Requirement Description	Priority
Standards **SO-17**	The Service Provider shall give an overview of how their current working practices align with ITIL v3 guidelines, and how they will align their service offering in this instance to ITIL v3 .	Must
Standards **SO-20**	The Service Provider shall list what industry recognised organisation wide Service Management related accreditations they have successfully achieved in the UK along with any expiry/renewal dates where relevant. Please note the Service Provider may be required to provide proof of such accreditations if successful/short listed.	Must
Working with TfL's Resolvers and Suppliers **SO-21**	TfL IM operates in a multi-source environment, working with various vendors and partners in the delivery of IM/IT services. The Service Provider shall demonstrate where they have worked successfully in a similar environment and what processes they intend to put in place to ensure a strong working relationship with all of TfL's partners and internal IM resolver groups?	Must
Training **SO-22**	The Service Provider shall describe its training and development plans to ensure that the right person has the right knowledge, at the right time to deliver and support the service/s, and how this will be maintained during the lifetime of the agreement.	Must
Training **SO-23**	The Service Provider shall outline what (if any) training they will require on TfL systems and applications for successful delivery of the service.	Must

Transport for London

Req Title	Requirement Description	Priority
Training **SO-24**	The Service Provider shall outline what training and learning material they would provide TfL to distribute to its staff on how to use the service. The training material provided must confirm to user manual standards followed by similar products. The Service Provider may be asked to update the learning material with reviews and comments from users at no extra cost.	Must

5.20.1. TfL Service Level Agreements (SLAs)

Severity	Definition	Target	Measured
1	• All or any part of the service is unavailable resulting in failure of business critical activities. Business critical activities include client services which cannot be mitigated (mitigation shall include the use of other available services); and/or • The incident affects the overall security of the TfL estate; and/or • The incident has a detrimental impact on the IM operations of TfL declared by designated individuals within TfL IM (IM Duty Managers (IMLT), Major Incident Managers, the IM Service Delivery Manager or the IM Security Manager). and/or • The incident affects users at a critical site or more than 50% of users across all sites.	Service is restored or a work-around is agreed **within 1 hour for 90%** of incidents and **within 2 hours for 98%** of incidents not resolved within 1 hour.	24 hours, 7 days a week, including public holidays

Transport for London

Severity	Definition	Target	Measured
2	Business activities are adversely affected resulting in some impact on business operations where; • The incident prevents at least one department from effectively performing key business activities; or • The incident causes a failure to redundant services that increases the risk to business critical activities.	Service is restored or a work-around is agreed **within 2 hours for 90%** of incidents and within **4 hours for 98%** of incidents not resolved within 1 hour.	24 hours, 7 days a week, including public holidays
3	Business activities are adversely affected resulting in some impact on business operations where: • The incident prevents users from effectively performing non key business activities; and/or • The Incident is limited in scope and scale. This includes equipment failures where due to redundancy and resilience, non-critical services are unaffected;	Service is restored or a work-around is agreed **within 8 hours for 90%** of incidents.	8:00 to 18:00, Monday to Friday, excluding public holidays.
4	• The service is not affected, e.g. queries; or • The incident affects a service component that has a dependency on support parties that are not managed by TfL IM; and/or • The incident affects a service component that cannot be fully supported	Reasonable endeavours only.	SLA not measured.

5.21. Service Related: Service Transition requirements

Req Title	Requirement Description	Priority

Transport for London

Req Title	Requirement Description	Priority

Service Transition
 	
ST-01
	Prior to take on of service into support, TfL require completion of a TfL Service Support Model document. The Service Provider shall be required to enter into discussions to assist drafting and agreeing this Service Support Model document.
	This document shall describe:
	
	   o The final service solution, support organisation, support responsibilities and the relevant support processes of parties involved in the delivery of the service / solution.
	   o How the service provider will interact at an operational level with TfL's existing service providers (internal and external) for the management of incidents, requests, releases and changes.
	   o How all support parties (TfL suppliers and other third parties) will deliver services to support the final solution.
		Must

Service Transition
 	
ST-02
	The Service Support Model is to be completed before service is handed over and made operational.
	
	The Service Provider shall confirm:
	
	   i. Acceptance of this requirement.
	   ii. Their active participation in discussions to draft, document and approve the final Service Support Model document.
	   iii. Allocation of necessary resources to assist with production and acceptance of this document.
	   iv. Representation of this task within the Service Provider's high level project plan
	
	Arqiva is to confirm acceptance of this requirement or propose alternative approaches.
		Must

Transport for London

Req Title	Requirement Description	Priority

Service Transition
 	
ST-03
	The Service Provider shall detail their transition approach including, but not limited to the following areas:
	
	   o Compliance with TfL Pathway, a PRINCE 2 project management methodology.
	   o Project plan and milestones
	   o Resource plan
	   o Dependencies and TfL obligations/support during transition
	   o Caveats, Assumptions, Risks and Issues
	   o Configuration management
	   o Data migration
	   o Knowledge/skills transfer
	   o Training and communication
	
	The above should include both initial take on of the service and any subsequent refreshes or upgrades that the Arqiva envisages as taking place during the lifetime of the Agreement.
		Must

Service Transition **ST-04**	The Service Provider shall describe their approach to Service Transition and any toolsets used with respect to the deployment process.	Must

Service Transition
 	
ST-05
	TfL requires a range of technical support material to be produced as part of service transition into live support, these include documents such as:
	
	   • Operations Manual;
	   • FAQs;
	   • Known Errors (defect log);
	   • Service Desk scripts;
	   • Service Catalogue entries;
	   • First Line Support Troubleshooting Guide;
	   • Details of Administration / Housekeeping / Maintenance / Periodic Activities to be delivered by TfL support teams
	
	Please demonstrate how your solution will achieve this objective
		Must

Transport for London

5.22. Service Related: Service Level Management

Req Title	Requirement Description	Priority
Support Hours **SL-01**	The Service Provider shall confirm that they will be able to support the system on a 24 x 7 basis, including Public Holidays. If the Service Provider are unable to meet this requirement they are asked to suggest alternative support hours along with their rationale for proposing these support times The Service Provider shall outline what level of support they will provide outside of the core business hours.	Must
Service Targets/Levels **SL-02**	All Service Level Agreements (SLAs) shall meet the minimum TfL requirements. The Service Provider shall confirm that they can comply with the service levels or, if appropriate, suggest alternatives. The Service Provider shall implement SLAs commensurate with each of the areas of service responsibility that will be undertaken. These SLAs will be aligned to requirements detailed within this ITT. The Service Provider shall will take part in discussions to have these agreed and documented within a Service Support Model. The Service Provider shall confirm acceptance of this requirement or propose alternative approaches. The Service Provider is expected to meet regularly with designated TfL contact to review the service and performance How will service levels be measured and reported on? What plans and actions will the Service Provider undertake if performance drops below agreed service levels?	Must

Operational Level Agreements
 	
SL-03
	The Service Provider shall maintain Operational Level Agreements (OLAs) with their appropriate resolver groups for management of incidents to ensure expectations on incident response and resolution times are met. The Service Provider shall describe how such operational interfaces would be defined, agreed and implemented covering areas such as:
	   o How the service on both sides of the interface will be monitored, including the exchange of status information;
	   o How the two organisations will cooperate to identify the causes of any faults, particularly where it is not immediately clear on which side of the service boundary the fault lies;
	   o Escalation processes to ensure that the appropriate technical resources are available and applied to rectifying service issues.
	
	   o The Service Provider shall take part in discussions to have these agreed and documented within a Service Support Model. The Service Provider is to confirm acceptance of this requirement or propose alternative approaches.
		Must

Transport for London

5.23. Service Related: Service Assurance

Req Title	Requirement Description	Priority
Use of TfL Tools **AS-01**	TfL uses BMC Remedy as its standard Service Management tool. The Service Provider should document how integration with Remedy will be achieved, where it has been utilised previously and what training requirements the Service Provider anticipates it will require. If the Service Provider has not utilised Remedy previously, they should demonstrate where they have integrated another IT Service management tool.	Must

Performance Monitoring
 	
AS-02
	The Service Provider shall identify:
	   o Any third parties and preferred suppliers that they propose to use to deliver the Solution / Services.
	   o For each third party identified above, the Service Provider shall provide a brief description and the third parties' involvement within the proposed solution.
	   o For each third party identified above, the Service Provider is to provide a brief description of where this relationship has been previously applied.
		Must

Performance Monitoring
 	
AS-03
	The Service Provider shall be responsible for:
	   o Advising TfL of any technical developments or products and services that will or may have an impact on any aspect of the services;
	   o Providing reports to TfL on the performance against service level targets;
	   o Attending regular Supplier Management meetings;
	   o Participating in corporate IM service reviews.
	The Service Provider shall take part in discussions to have the content and frequency of performance reporting agreed and documented within a Service Support Model. The Service Provider is to confirm acceptance of this requirement or propose alternative approaches.
		Must

Performance Monitoring
 	
AS-04
	The Service Provider shall describe how it intends to:
	   o Continuously monitor service levels against the agreed targets.
	   o Implement a procedure for initiating corrective action when performance falls below the agreed service levels.
		Must

Transport for London

Req Title	Requirement Description	Priority
Performance Monitoring **AS-05**	The Service Provider shall provide an example of where it has previously implemented a Service Improvement Plan for a similar service to the one outlined in this tender and highlight the benefits that were gained from it	Must
Performance Monitoring **AS-06**	What plans and actions would the Service Provider undertake if performance drops below agreed service levels?	Must
Reporting **AS-07**	The Service Provider shall describe: o How it intends to report against service levels. o The frequency and method of delivering this report. The Service Provider shall take part in discussions to have the content and frequency of the performance reporting agreed and documented within a Service Support Model. The Service Provider shall confirm acceptance of this requirement or propose alternative approaches.	Must
Reporting **AS-08**	For Major Incidents (severity 1 or severity 2 – see Service Level Agreement) the Service Provider shall produce a major incident report within three days detailing: o Findings of incident investigation o Immediate resolution o Long term fix o Actions to avoid/minimise reoccurrence.	Must
Reporting **AS-09**	The Service Provider shall confirm that it shall provide all reporting on a TfL periodic basis, each period consisting of 4 weeks and each year consisting of 13 periods.	Must

Transport for London

Req Title	Requirement Description	Priority
Service Reviews **AS-10**	The Service Provider's Account Manager shall meet with representatives of TfL IM Supplier Performance & Assurance and any other relevant TfL team on a monthly/periodic basis at a location to be specified by TfL. Topics to be covered within the service review meeting will include: o Service Provider performance against SLAs. o Any service issues and incidents not met within SLA and the proposed remedial work. o Any proposed changes to the service. o Product roadmaps. o Invoicing/payment. o Any other issues or opportunities.	Must
Service Reviews **AS-11**	The Service Provider shall outline their approach to service review meetings, and describe how they would undertake them with TfL.	Must
Service Reviews **AS-12**	The Service Provider shall provide a proposed Organisational chart of their Account Management/Senior Management structure, outlining roles and responsibilities that would be involved in delivering the service.	Must
Service Reviews **AS-13**	TfL IM operates in a multi-source environment, working with various vendors and partners in the delivery of IM/IT services. The Service Provider shall demonstrate where they have worked successfully in a similar environment and what processes they intend to put in place to ensure a strong working relationship with all of TfL's partners.	Must
Escalations **AS-14**	The Service Provider shall outline their proposed escalation process, including timeframes in between hierarchical escalations and response times.	Must

5.24.   Service Related: Service Testing

Transport for London

Req Title	Requirement Description	Priority
Testing **TT-01**	The Service Provider shall carryout testing of the System and associated Services during the implementation phase and maintenance phase as described by Schedule 6 (Testing Regime). As per section 1.2 of schedule 6, please outline the testing process, including testing phases, to be carried out to ensure that the Functional and Non Functional requirements described by Schedule 4 (SoR) are met,	Must
Testing **TT-02**	To support a structured approach to testing, the Service Provider shall produce various documents as per the agreed project schedule. These documents consist of Test Strategy, Test Plans and Test Specifications as set out in section 1.2.1 of Schedule 6.	Must
Testing **TT-03**	Prior to system go live, the service provider shall ensure that Simulated Operational Testing is performed in order to simulate and prove that the Operational Services have been met. This includes demonstration of the following: a. All Hardware in its final location; b. Software is ready to be used operationally; c. Relevant TfL Personnel who make use of the system have been appropriately trained in the operational processes and procedures to be employed using the System; and d. All Service Management processes are in place and understood by relevant personal Please provide details of how this testing will be carried out	Must

Transport for London

Req Title	Requirement Description	Priority

Testing
 	
TT-04
	Please provide detail of the quality management tools and processes to be used in Testing including:
	
	  a) the standards to be applied to Testing;
	
	  b) Test design techniques to be employed during the Testing;
	
	  c) requirement traceability mechanisms;
	
	  d) Defect management processes;
	
	  e) Defect categories and Resolution processes;
	
	Please provide details of how this testing will be carried out
		Must

Transport for London

Req Title	Requirement Description	Priority
Testing **TT-05**	The Service Provider shall, in order to test requirements with other third parties or systems co-operate with and enter into dialogue with Other Service Providers in relation to testing. This includes a) develop a detailed timetable for all relevant end to end integration Testing; b) develop Test Plans and Test Specifications for integration Testing, including all actions to be performed, jointly or individually with associated expected results, that will together constitute the agreed integration Test; c) update all defects arising from integration Testing in the incident log, including those currently assigned to TfL or Other Service Providers for resolution; d) report on the progress of integration testing and the generation of Interoperability Test reports which shall include obtaining Data from the Other Service Providers as required; e) generate final Interoperability Test reports, which shall include obtaining Data from the Other Service Providers as required and detailing outstanding Incidents and assigning responsibility for Resolution to the relevant Other Service Providers if appropriate f) Use of legacy or migrated data when carrying out end to end testing to demonstrate that Legacy Data is correctly transferred to and stored Please provide detail of how integration testing will be managed maximum	Must
Testing **TT-06**	Test witnessing; As set out in section 1.2.5 of Schedule 6 (Testing), TfL may request that its employees, agents or sub-contractors witness any of the Implementation Phase Testing, and the Service Provider shall comply with such request. Testing may be witnessed either on-site or by the use of remote facilities, whichever is most appropriate to the Test and as agreed with TfL. This includes: Please confirm this can meet, or any limitations TfL needs to be aware of,	Must

Transport for London

Req Title	Requirement Description	Priority
Testing **TT-07**	The Service Provider shall be required to perform Regression Testing as necessary to demonstrate that changes to the Software have no adverse impact on the System, Interfaces, the Other Service Provider systems or any Hardware, Software or systems Please provide outline of how regression testing will be carried out.	Must

Testing
 	
TT-08
	The Service Provider shall appoint a Test Manager as soon as reasonably possible.
	
	The Service Provider shall ensure that its Test Manager:
	
	a) is responsible for managing the Service Provider's obligations under Schedule 6;
	
	b) will on a regular basis, liaise with TfL's Test Assurance Manager (and in any event on a daily basis) during each test, including in relation to:
	
	    a. co-ordinating the development and Approval of the:
	
	        i. Implementation Test Strategy;
	
	        ii. Test Plans
	
	        iii. Test Specifications; and
	
	        iv. Test reports;
	
	c) planning the development of the required Tests in the Implementation Phase;
	
	d) co-ordinating the implementation of all Tests and their execution; and
	
	e) monitoring and reporting on progress of all Tests in accordance with this Schedule 6.
	
	Please provide an overview of the testing organisation for this project,
		Must

Transport for London

Req Title	Requirement Description	Priority

Testing
 	
TT-09
	The Service provider shall ensure that releases, during the implementation phase and maintenance phases are tested to ensure that the software meets the requirements:
	
	Please provide a description of your proposed approach to Testing releases throughout the Maintenance phase due to change(s) resulting from:
	
	    a) System Requirement(s) updates;
	
	    b) Incident(s);
	
	    c) Standard version upgrades; and
	
	    d) Patch releases
	
	Your answer should describe how such releases, will in accordance schedule 6, section 1.2.4, demonstrate to TfL that each software and configuration release:
	
	    1. is in accordance with the design documents and the relevant Test Specification;
	
	    2. is consistent with the agreed Change Request;
	
	    3. is consistent with the Service Levels;
	
	    4. is implemented in accordance with good industry practice; and
	
	    5. Issue resolution method, cost and timescales;
	
	Please provide an overview of the testing organisation for this project
		Must

Transport for London

6. Scenarios

6.1. CentreComm Bus Incident – Passenger Illness

This scenario is usually handled by the first line Operator (ERT) as there is usually no impact on service;

- Passenger taken ill on the bus so the bus driver initiates a radio call to CentreComm.

- An Operator (ERT) creates a new Incident, records the bus details based on information displayed on the IBus map (a separate system available to the Operator).

- Details of the call are captured from the bus driver by the Operator, e.g.:

  o Whether the passenger is conscious and breathing, nature of the illness / symptoms (e.g. chest pain, dizziness) and approx age of the passenger & gender.

- The Operator will verbally confirm the location of the bus and will geo-locate the Incident on the map.

- If emergency assistance is required, the Operator will call the required emergency services (e.g. London Ambulance Service) and pass them the details of the Incident including the CentreComm Incident Reference.

- The Operator will call back the bus driver to confirm that the emergency services have been notified.

- Bus driver calls CentreComm to provide an update that the emergency services have attended the scene and the passenger has been taken to hospital.

- The Operator records the details of the update from the bus driver and confirms that the Incident has now cleared.

6.2. Bus Incident – Road Traffic Accident (RTA)

This scenario is usually handled by the first line Operator (ERT) initially then passed across to the NRT Operator Incident Queue as an impact on service is anticipated. An Operator can continue to update an Incident with call details as the NRT is assigning a Resource.

- Bus involved in an RTA (Road Traffic Accident).

- The ERT Operator creates a new Incident, records the bus details based on information displayed on the IBus map.

- Details of the call are captured from the bus driver by the ERT Operator, e.g.:

  o Whether there are any injured parties (passengers, other drivers, pedestrians), nature of the injuries if applicable including details of the persons injured (approx age, gender)

  o Whether the Bus is unfit to continue in service, if so, an NRT response is required.

- The Operator will verbally confirm the location of the bus and will geo-locate the Incident on the map.

- If emergency assistance is required the Operator will call the required emergency services (e.g. London Ambulance Service, Met Police) and pass them the details of the Incident including the CentreComm Incident Reference.

- The Operator will confirm to the bus driver when the emergency services have been notified. The Operator will request that the driver calls back when the Incident has been attended by the emergency services and / or is cleared.

Transport for London

- Bus driver calls CentreComm to provide an update that the emergency services and / or Resource have attended the scene.

- Operator accesses NRT Incident Queue, reviews the Incident and assigns a Resource.

- Resource calls CentreComm to advise that they are now at the scene, Resource calls CentreComm to advise clearance of the Incident.

6.3. Ticket Acceptance for Centrecomm

South West Trains (a TOC) calls Centrecomm to request that their train ticket be accepted on buses between Surbiton and Wimbledon due to a signal failure stopping all trains.

The Operator creates a Ticket Request, and sends the Ticket Request number via,

- an SMS to affected Bus Operators,

- post to the Bulletin Boardwith full detail of ticket acceptance, and

- a radio broadcast to the bus drivers.

The bus drivers need the three (3) digit Ticket Request number to enter in their ticket machines for any ticket acceptance passengers.

CentreComm raise a request to LU or the TOCs for ticket acceptance for bus passengers when there is a service issue.

6.4. Implementing a Diversion

An incident triggers a need for a Diversion to be implemented immediately.

As an immediate measure, CentreComm re-directs the route down roads where existing bus routes travel (as a risk assessment has already been completed, and the route will be safe for buses).

CentreComm will communicate the Diversion;

- an SMS to affected Bus Operators,

- post to the Bulletin Boardwith full detail of Diversion, and

- a radio broadcast to the bus drivers.

An NTC Resource is dispatched to the area to risk assess a more suitable route for bus traffic. The NTC Resource and Centrecomm will discuss and agree by phone a revised diversion route.

CentreComm will communicate the revised diversion details again, repeating the above comms.

The Diversion Reference Number is used by the Bus Operators, when quoting any shortfall in their targets caused by a Diversion.

See also Live Information Desk (LID) scenario below.

6.5. LU Network Incident

The LUCC take a call notifying a person under a train in a station.

An Operator, e.g. the Incident Desk Controller, will create an Incident and assign the Incident Type, which will pre-populate the Action List.

Transport for London

Multiple TfL LUCC desk staff will simultaneously respond to the incident, using an Incident Activity Template where appropriate for each action taken, or information received.

Each action will create an incident log entry. As the incident progresses and actions taken, the Incident log expands. The dashboard for the Incident will show completion status of the Action List.

For example, the following activities will be created as Action List types;

- NIRM deployed, including time,

- NIRM on site, including time,

- CAT1 implemented, including time

- Stalled train, record train Number, start time, then update with cleared time,

- Suspension of service, including start time

- Passenger service started (this is the same as end of suspension of service)

- Declare move from "Severe delays" to "Minor delays", (this is decided jointly between the LUCC NIM and the line control,

- Declare move form "Minor delays" to "Good service"

If the Incident impacts on service, the Operator NIM (Network Information Manager) will send out a message to the network indicating a delay to service.

The LUCC will use the CUPiD Lost Customer Hours (LCH) calculator to get a rough order of magnitude of LCH.

The Line Service improvement team will write up the incident separately at end of shift in CUPiD.

6.6. LU Weather Readiness Plan

Contingency Planning set up Weather Readiness Plans for each line and business area that needs to invoke a Weather Readiness Plan.

The plan is invoked by LUCC when the weather forecast indicates there may be a problem. The LUCC may trigger the Weather Readiness Plan for any day of the plan, e.g. if a weather forecast indicates a problem emerging quickly, the plan may be initiated on Day 3, or a plan may stay on Day 3 for several days as the forecast changes.

The Service Control Managers are responsible for ensuring the Weather Readiness Plan status reporting is complete. This responsibility may be delegated.

Weather Readiness is reported in a hierarchy;

- Each line's / dept status for: Stations, Lines and, Service Control & Maintenance

In addition depts. (e.g. NOM/ SOO Asset Performance) report on; Staff welfare, Communications, for a series or action list of tasks entered by the responsible user.

The status is rolled up to; a line status, then,

- a network status,

Transport for London

only showing green when all components are green. This enables the LUCC to identify where action is outstanding.

6.7. LUCC Sending an Emergency Alert (currently via SIMlink)

A security situation develops at Victoria station, where the station has been evacuated and Underground trains have been instructed not to stop by the Met Police.

The LUCC send out a simultaneous Emergency Alert to all Line Control Centres.

Each recipient acknowledges receipt of the Emergency Alert.

If no acknowledgement is received, LUCC phones the Control Centre to pass the message.

6.8. LU Compiling and Invoking a Contingency Plan For An Event

The Contingency Planning team set up a Contingency Plan for Wembley stadium events for the summer.

The LUCC create a number of events for the calendar of events for Wembley stadium.

Each event will be associated with a contingency plan incidence. As the event nears, LUCC will start to complete the Action List.

The summary of the Event will show the completion status of the Action List activities, e.g.

- Day 7, check scheduling of trains,

- Day 5 Police briefing with other services,

- Day 1 (Day of event) Call round line managers to confirm OK,

Day 1 Call round affected stations to confirm OK.

6.9. LU Ticket Acceptance

First Capital Connect contact the Network Information Manager (NIM) and advise of signalling problems at London Bridge and request that their tickets are accepted on the London Underground via any reasonable route.

The NIM creates an incident which will pre-populate the action list.

BBMS (broadcast), ESUB and SMS text messages will be sent by the NIM/assisting Controller and the TfL Twitter team will be advised.

FCC later advises that acceptance is no longer required. NIM make a follow up connect broadcast, updates ESUB and sends SMS message.

NIM requests incident is reviewed for closure.

TSC reviews incident for closure.

NOM closes incident.

6.10. LU Category One Incident Declaration

A Cat1 (Category One) is declared as per the criteria described in Ref 10. The SOO decides and will declare a Cat1. FIM (Formal Incident Management) will be stood down when the Incident is deemed to be resolved and recovery is handed to the Line Controller to manage.

Transport for London

LUCC will get advised that service has resumed either from the Service Manager to the NOM or line information Manager (LIM) to the Network Information Manager NIM. The service will be resumed to a service status (Good Service, Minor Delays, Severe Delays)

6.11. CentreComm Live Information Desk (LID) operator sends out a twitter message

An incident triggers a need for a Diversion to be implemented immediately.

As an immediate measure, CentreComm re-directs the route down roads where existing bus routes travel (as a risk assessment has already been completed, and the route will be safe for buses).

The LID operator creates a Twitter message for the public.

The LID Operator updates the LID Desk Log with the detail of the Twitter feed published.

Note – as the Desk Logs are not extracted to CDR currently, the LID Desk Log will not be extracted.

7. Data required for CentreComm and LUCC

7.1. Reference data

The following reference data must be maintainable via an Admin function.

Field	Example values – to be maintained by an admin user	CentreComm?	LUCC?
Asset Type	E.g Escalator, lift, bridge. Note this is to assist the LUCC in identifying similar incidents. Could link to an asset register in future.	Not relevant	Relevant
Bus route alternative	Drop down values if no bus route indicated; e.g Rail replacement Light running Out of service running	Relevant	Not Relevant
CAT One Declared Reason	Category One must be declared if there is the potential (as of Issue 4) for .e.g ; • Trains to be stalled for more than 30 minutes or • More than one line, multiple locations to be affected. Or for • A radio system failure, • Major power failure, • An evacuation of the Underground, • A person under a train.	Not relevant	Relevant
Control Centre Desk Log Type	E.g. Phone call, staff on duty change, LID entry	Relevant	Relevant

Transport for London

Field	Example values – to be maintained by an admin user	CentreComm?	LUCC?
Diversion Cause Codes	E.g. Roadworks Burst water main	Relevant	Not relevant
Duty	See ref 14 for examples of data	Relevant	Not relevant
Duty Areas	See ref 14 for examples of data	Relevant	Not relevant
Duty Turns	See ref 14 for examples of data	Relevant	Not relevant
Incident / Event Type	E.g. Signal failure, Wembley event, O2 event, points failure, bridge strike, lift failure Also known as Cause Code in Centrecomm Sample LUCC incident types: AMB (ambulance request) COM (Communications Failure) DRC (Derailment/Collision) DUR (Duress alarm) EVN (Event) EXT (External to LU)	Same as Event Category Relevant	Relevant
Incident Origin	E.g. Bus driver, Police, London Ambulance Service (LAS)	Relevant	Relevant
Notification Route	E.g Phone, Fax, Email	Relevant	Relevant
Info Source	E.g Line Control Centre, station staff, Emergency services	Relevant	Relevant
Location Directory	Include but are not limited to; • Location Alias (i.e. the location abbreviation or code including HLUL code) • Location Name (e.g. Victoria station, VIC, VICS), • Short code • Grid reference/Coordinates (e.g. Easting and Northing), • Control area, • Line (e.g. Victoria), • Owner (e.g. VIC), • Post Code (e.g. SW1E 5ND), Longitude and Latitude.	Not relevant	Relevant

Transport for London

Field	Example values – to be maintained by an admin user	CentreComm?	LUCC?
LU station	Include but are not limited to; Name Short code, e.g; HLJ, GLR, UPB STA TOH FIR Zone (s)	Not relevant	Relevant
Operator garage	Associated with route	Relevant	Not relevant
Resource type	E.g NTC, Bus Station Controller, Infrastructure Controller, Truck, cleaner	R4.8.03	Not relevant
SMS / Email Message Type	E.g Service status message, OTP updates, Step-free updates	Relevant	Relevant
Ticket Request Authorisers	Users with authority	Relevant	Not relevant
Ticket Request Causes		Relevant	Not relevant
Ticket Request Origins		Relevant	Not relevant
SMS/ email Distribution Groups		Relevant	Relevant
Commonly used links	The following list is for illustration purposes only: 1. CentreComm Sharepoint: http://collab/st_/cco/default.aspx 2. LU Status: http://nccstatus.lul.co.uk/ 3. LU CC: http://luintranet.tfl/Ops_maintenance/Service_Support/643.html 4. Trackernet: http://trackernet.lul.co.uk/ 5. Countdown: http://countdown.tfl.gov.uk/ 6. National Rail: http://www.nationalrail.co.uk/ 7. Google maps:	Relevant	Relevant

7.2. Incident status

LUCC	Open	Closed / Cleared
CentreComm	Initiated	Cleared

CentreComm – When an Incident is re-opened the Status should be set to OPEN>INITIATED.

Transport for London

Status	Progress Status	Rules	Current Colour Code (for guidance only)
Open	INITIATED	Automatically set when incident is created	Black
Open	NRT	Automatically set when incident is assigned to an NRT for further action	Red
Open	MONITORED	Manually set by an NRT	Pink
Open	RESOURCE-AT-SCENE	Manually set by an NRT	Blue
Open	RESOURCE-ASSIGNED	Manually set by an NRT	Mauve
Closed	CLEARED	Manually set by an operator when incident complete	Green

7.3. Incident data

Field	Description	Centrecomm?	In extract? Order	LUCC?
Incident Reference Number	Daily counter Reference number This must be a maximum of 4 digits long; the Operator does not wish to dictate a long number which could be more prone to error. (The current CentreComm system starts at '1' at midnight, incrementing with each incident, until 23:59.)	System generated	Yes	System generated
Internal ID for incident	System reference number	System generated	Yes 4	
Incident start time	Time incident started, could be different from time notified to control centre	Default to Incident notified time, editable	Yes 1 4	Default to Incident notified time, editable
Incident end time	Incident end date timestamp		Yes 15	
Incident notified time	Time incident called into control centre and logged into solution	System generated		System generated
Creation date time stamp	Incident creation date, from audit trail	System generated, not editable	Yes 1	

Transport for London

Field	Description	Centrecomm?	In extract? Order	LUCC?
Last updated date	Last edited, from audit trail	System generated, not editable	Yes 2	
Incident Type	Also known as Cause Code in Centrecomm Drop down list; dictates type of Action List displayed	Mandatory	Yes 6	Mandatory
Incident type description	Narrative of incident type Derived from Incident type selected	Display	Yes 7	Display
Route	Bus Route number of the Bus making the call to CentreComm. Validated against CDR data, non-route data accepted	Optional	Yes 21	Not relevant
Garage	Garage that bus route belongs to. Auto-populated when the route is selected.	Optional	Yes 22	
Running Number	Available on iBus screen, entered by the Operator. Free text	Optional	Yes 12	Not relevant
Bonnet Number	Available on iBus screen entered by the Operator. Free text	Optional	Yes 13	Not relevant
Location	'Easting' and 'Northing' An Incident will be manually geocoded	Mandatory	Yes Easting 19 Northing 20	Optional
Street	Location of the Incident. The list of Streets on the Line of Route will be displayed for selection or can be free text	Mandatory	Yes 16	Optional

30/03/2015

Transport for London

Field	Description	Centrecomm?	In extract? Order	LUCC?
Junction	Location of Incident and relative location to a Junction. The list of junctions on a street will be displayed for selection Or can be free text	Mandatory	Yes 17	Optional
Postal Area / Post Code	Geocoded Post Code based on the Incident location selected on the map by the Operator.	Mandatory	Yes 18	Optional
Direction	Direction of travel of the Bus.	Optional	No	Not relevant
Incident Headline	Summary on incident, free text Spell check Used in summary reporting	Optional, default to Incident type code (prev Cause Code + Incident Type narrative)	Yes 5	Mandatory
Incident Origin	Source of the Incident – who raised it. Drop down list	Mandatory, specific to Centrecomm, default to "Bus driver	Yes 8	Mandatory, specific to LUCC
Incident origin description	Narrative of the source of the incident Display, derived from Incident Origin	Display	Yes 9	Display
Incident Description	Fuller description of the Incident and details captured Free text Spell check	Optional	Yes 3	Optional
MPS CAD Reference	Police reference number.	Optional	Yes 10	Action list item
Ambulance Reference	Ambulance reference number Free text	Optional	No	Action list item
Fire Brigade Reference	Fire brigade reference number Free text	Optional	Yes 11	Action list item

Transport for London

Field	Description	Centrecomm?	In extract? Order	LUCC?
Office of Rail Regulation (ORR) reference	ORR Reference Free text	Not relevant		Optional
Other Reference	Free format text – no validation.	Optional	No	Optional
Police Attended	Flag to indicate Police have attended scene. Recorded via an Action list item by LUCC	Optional R4.1.1.007	No	Action list item
Ambulance Attended	Flag to indicate Ambulance have attended scene. Recorded via an Action list item by LUCC	Optional R4.1.1.007	No	Action list item
Fire Brigade Attended	Flag to indicate Fire brigade have attended scene. Recorded via an Action list item by LUCC	Optional R4.1.1.007	No	Action list item
EIRF number associated	Incident details recorded for LU post-event by line controller in EIRF for analysis and follow up	Not relevant	No	Optional
Other Reference Attended	Flag to indicate Other have attended scene.	Optional	No	Optional
Status	An Incident may have a number of Status	Mandatory, specific to Centrecomm	No	Mandatory, specific to LUCC
Flags	An Incident may have the following Flags set	Optional, e.g. "Notify to Duty Manager" R4.1.1.020, Diversion Assigned		TBC
LU Line	LU line where incident occurred, needs entered, a station can be on multiple lines Drop down	Not relevant	No	Required

Transport for London

Field	Description	Centrecomm?	In extract? Order	LUCC?
LU Station	LU Station where incident occurred Drop down, use short codes	Not relevant	No	Optional, Mandatory for a Cat 1
Asset type	Asset type associated with incident Drop down	Not relevant	no	The solution could link to Asset Register However there are currently < 10 incident/ day that involve an asset and the EIRF record raised post-incident by the line controller will link to Ellipse
Asset reference	Asset reference if known	Not relevant	*no*	*Optional*
Linked List	Numbers of all linked (associated) Incidents, multiple occurrences. Shows that an incident is linked with one or more incidents	optional	Yes 23	optional
Incident Activity	Each update or follow up. Creates narrative of incident as it unfolds. Multiple entries possible.	Optional	No	Optional
Action list	A set of actions dependant on the incident type selected.	Not relevant	No	Optional
Incident attributable to..	Drop down (Other Asset PUT PIOT Ops)	Not relevant	No	Mandatory for a Cat 1
Informed	Free text description of who CentreComm operator has spoken to - no spellcheck required	Relevant	No	Not relevant

Transport for London

7.4. Message templates

Message templates, including but not limited to;

Field	Description
Message type	The message template type e.g. "Delay"
Message text	Standard text for a message template, will include variable fields inserted from originating incident / diversion
Relevant to	Which control centre has visibility, access to and update rights
Message tags	Drop down list of relevant tags, to enable faster search on message templates and messages sent.

7.5. Desk Log Data

Control Centre Desk Log details will include, but will not be limited to:

Field	Description	Centrecomm?	LUCC?
Log Reference	Unique Reference ID for a log	System generated	System generated
Log type	Drop down	Required	Required
Creation date and time	Default to the current date and time. The user will be able to amend the date / time,	System generated	System generated
Headline description / title		Revelant	Required
Reporter	User ID of Desk Log entry creator	Revelant	System generated
Location	Where the note relates to	Revelant	Optional
Description	Free text with spell check	Revelant	Optional
Control Area/Line	Drop down	Not relevant	Optional

7.6. Ticket Request Log Data

CentreComm receive Ticket Requests; either from LU or a TOC Tramlink, DLR and London Overground

LUCC can;

- make a ticket request to the buses or a TOC as a result of an incident, will record detail as part of incident,

Transport for London

- receive a ticket request from a TOC or from the buses, (via Centrecomm, very rarely) Will record as need to ;

  o send out staff message so CSAs at station know to accept tickets and,

  o make customer announcements.

Field	Description	Centrecomm?	LUCC?
Inbound LU and TOC ticket request to Surface (CentreComm)		Relevant	
Direction	OTP – Other Transport Provider (Inbound to LUCC and CentreComm)	Both OTP and Outbound (occasionally)	Both OTP and Outbound
Ticket Request Pre-Pay Number	The pre-pay number must be in the range 101 – 999 (inclusive) due to limitations on the ticket machines used by Buses. Once 999 is reached, the number should restart at 101.	Relevant	Not relevant
Origin of incident	LU TOC Train Operating Company	Relevant	Relevant
Valid time on	A Ticket "Valid on time" may be before the current time.	Relevant	Relevant
Valid time off		Relevant	Relevant
Location of incident		Relevant	Relevant
Reason for Ticket holder request		Relevant	Relevant
Lines affected		Relevant	Relevant
Between stations		Relevant	Relevant
Incident start time		Relevant	Relevant
Cleared Time		Relevant	Relevant
TOC only			Relevant
TOC Code – from list of codes			Relevant
Raised by - from list of authorised sources			n/a
Contact No.- defaulted from Raised by			n/a
Incident Code & Description			n/a
Cleared auth by			n/a
General remarks			n/a
Estimate duration			n/a

Transport for London

7.7. Diversion – CentreComm only Data

Diversion details will include, but will not be limited to (CentreComm Req R4.3.01):

Field	Description	Extracted? Order in extract
Diversion Reference Number	This must take the format of a 5 digit reference number, commencing with a letter 'D'. (i.e. in the format Dxxxxx).	Yes 1
Logged date	System generated	Yes 2
Last modified date	System generated	Yes 3
Start date time	Start date timestamp of diversion	Yes 4
End date time	End date timestamp of diversion	Yes 5
Status of diversion	Drop of valid values	Yes 6
Network Operations Area	Drop down	Yes 7
Street name location	Free text	Yes 8
Junction location	Free text	Yes 9
Direction of diversion	Drop down	Yes 10
Comments	Textual	Yes 11
Description of diversion	Detailed description of diversion	Yes 12
(Diversion) Cause Code	Drop down	Yes 13
Cause description	Auto-populated from diversion cause code	Yes 14
Affected Routes	Drop down from valid valueswith option to add free text	No
Bus routes affected narrative	Free text description of bus routes affected by diversion	Yes 15
A list of one or more polygons defining the areas affected by the diversion.	Location (x & y coordinates, geocoded location point, street, junction, Postal Area Code)	Yes 16
Risk Assessed by	Free text	No

7.8. Notice Of Event Data

An Event is a planned occurrence that has some impact on the Bus Network (e.g. a Bus Route that is affected by a planned road closure). Events are notified to CentreComm via Notice of Events (NOEs) that are currently stored as Word documents on the CentreComm Sharepoint Site.

Transport for London

Note: These Fields are taken from the NOE Sharepoint solution. The fields will need to be re-validated against the final Sharepoint solution when the detailed design is completed.

Field	Description	Type	Nullable
NOE Reference	Reference Number of the NOE	varchar(255)	N/A
Documentation Link	Field to link (hyperlink) to the Sharepoint Site	varchar(255)	N/A
Status	Status of the Event	varchar(255)	N/A
Street (Main Location)	Location of the Event.	Varchar(255)	N/A
Junction	Location of Incident and relative location to a Junction.	Varchar(255)	N/A
Postal Area / Post Code	Post Code of the Event location.	Varchar(255)	N/A
Borough	Borough where the event is taking place.	Varchar(255)	N/A
Region	Region Code	varchar(255)	N/A
Effect of Event	Details of the event.	Varchar(255)	N/A
Start Date	Event Start Date	Date	N/A
Start Time	Event Start Time	Time	N/A
End Date	Event End Date	Date	N/A
End Time	Event End Time	Time	N/A
Cause	Event Cause / category	varchar(255)	N/A
Risk Assessment	Identifies if a Risk Assessment is required.	Varchar(255)	N/A
Routes Affected	List of affected Bus Routes.	Varchar(255)	N/A
SMR	Senior manager	varchar(255)	N/A
Duration	Event duration.	Varchar(255)	N/A
Description	Description of the Event.	Varchar(2000)	N/A
Diversion	Statement on whether a Diversion needs to be created.	Varchar(255)	N/A

Transport for London

Field	Description	Type	Nullable
Required			
Title	Title of the Event	Varchar(255)	N/A
Security Classification	Security classification of the Event	Varchar(255)	N/A
Reason for Late Notice	Reason for late notice of Event	varchar(255)	N/A
Reason	Reason description.	Varchar(2000)	N/A
Bus Stop	Bus Stop reference(s).	varchar(255)	N/A

Transport for London

7.9. Map Layer Data- Detail

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Area layers; • LoHAC areas and roads • GLA boundary • Low Emission Zone • Congestion charging Zone • SCOOT programme regions • Borough boundaries	Series of co-ordinates plotted	CentreComm	TfL – CDR	Should	Semi-annual	Last retrieved date	
Borough boundaries	Series of co-ordinates plotted	CentreComm	TfL – CDR	Should	Semi-annual	n/a	n/a
Bus information Toggle button for each type; • Bus Lane enforcement cameras (mobile) • Bus Lane enforcement cameras (static) • Counting Loop • Bus garage	X, Y co-ordinates	CentreComm	TfL – CDR	Must	Semi-annual		• Site NO • Type • Description • Status • Location (text) • Status flags • Bus routes Link to live Site Fault Management info for asset

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Bus Routes Note route records / streets traversed are also held as textual description	geo-spatial object	CentreComm	TfL – CDR	Must	Weekly	See full data	• Route number • Run number • Direction • AMOS sequence number • ITN no of each street traversed
Bus Routes turning points NB Turning Points are text data, a list of locations where a bus is authorised to finish short of its original destination.	X, Y co-ordinates	CentreComm	TfL – CDR	Must	weekly	See full data	• Bus Route turning point Id • Turning point number • Turning point location • Stand code • Stand description • Reliefs • General operation • Usage • Dest Text • Ferry vehicles Restrictions

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Bus Shelter	Easting Northing	CentreComm	TfL – CDR	Must	Semi-annual	As full data	• (Busnet) Stop code • Site name • Stop name • Stop location description (narrative) • Status • BODS code • Point Letter • Stop type (e.g. Stop – bus compulsory) • Easting • Northing

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Bus stop	Easting Northing	CentreComm	TfL – CDR	Must	weekly	Routes • Busnet) Stop code • Site name • Stop name • Stop location description (narrative) • Towards narrative • Status • Point Letter • Stop type (e.g. Stop – bus compulsory) • Easting • Northing	• (Busnet) Stop code • Site name • Stop name • Stop location description (narrative) • Status • Point Letter • Stop type (e.g. Stop – bus compulsory) • Easting • Northing

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
CCTV camera	Easting Northing	CentreComm LUCC	TfL – CDR	Must	Semi-annual	Camera number (CCTV Site number)	• Site No • Type • Desc • Status • Location (narrative) • Status flags • Bus routes Link to current faults
Connect radio holders		LUCC	Connect	Could	Dynamic	TBC in future	TBC in future
Court locations	X, Y co-ordinates	CentreComm	External data set	Should	Semi-annual	• Name • Address	• Name • address
Diversions	X, Y co-ordinate of centre of diversion	CentreComm	MICCS Solution	Could	Dynamic	• Diversion reference number • Start date and time • End date and time • Status • Street name location • Cause code	As data description

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Emergency Response Units for the LU network		LUCC	Masternaut application	Could	Dynamic	TBC in future	TBC in future
Events (Dynamic)	Easting / northing	Both	MICCS Solution	Must	Dynamic	• Incident Reference Number • Incident start time • Incident type • Bus Route • Location • Incident headline	As data description
Incidents (Dynamic)	Easting / northing	Both	MICCS Solution	Must	Dynamic	• Incident Reference Number • Incident start time • Incident type • Bus Route • Location • Incident headline	As data description
Landmarks: hospitals, medical centre	As data source	CentreComm	External	Should	Semi-annual	As available from 3rd party source	
Low Bridges	Easting / northing	CentreComm	TfL – CDR	Must	Semi-annual	Bridge height in metric and in imperial	

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
LUL Network (LUL track route)	Easting / northing	CentreComm LUCC	TfL – LUL	Must	Semi-annual	Station name Line name	
LUL Stations	Easting / northing	CentreComm LUCC	TfL – CDR	Must	Semi-annual	Station name Line name	
National Rail Stations (may be included on base map layers)	Easting / northing	CentreComm LUCC	External	Must	Semi annual	Station name Line name	
Nightclubs, Pubs, Bars etc. TfL may procure a corporate licence for access to this data	AS data source	CentreComm	External	Should	Semi-annual	As available from 3rd party source	
Notice of Events (loaded from Sharepoint)	Easting / northing	CentreComm	Solution / TfL CDR	Must	Dynamic	Start and end Dates Description Route(s) affected	See above
Post office	Easting / northing	CentreComm	External	Should	Semi-annual	As available from 3rd party source	
Railway bridges	Easting Northings	LUCC	LU intranet	Must	Semi-annual	Line name Location description	

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Resources	Easting / northing	CentreComm	MICCS Solution	Must	Dynamic	• Resource type • Resource name • Badge No • Logged in time • Available/ not available	As data description
Road network layers; o Transport for London Road Network (TLRN) • Boroughs resilience Network • Borough Principal Road Network • TfL Resilience Network • Strategic Road Network • Public Service Agreement Routes • Cycle Highways • Corridor Evaluation Framework	X, Y co-ordinates	CentreComm	TfL – CDR	Must	Weekly	Last retrieved date	

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Roadwork information	X, Y co-ordinates	CentreComm	TfL – CDR	Must	Dynamic		
Signals (also known as ATS (Automatic Traffic Signals) Toggle button for each Signal Type	X, y co-ordinates	CentreComm	TfL – CDR	Must	weekly with option to refresh	As full data	• Site No • Type • Description • Status • Location (narrative) • Status flags • Bus routes • UTC groups • Link to live Site Fault Management info for asset. .

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
TIMS (Traffic Information Management System) online	Eastings and northings (using Oracle Spatial coordinate system reference id SRID=81989) and Longitude / Latitude (WGS 84 aligned to Google Maps) coordinates	CentreComm	http://www.tfl.gov.uk/cdn/static/cms/documents/tims-feed-technical-specification.pdf TfL open data if not available in CDR	Must	5 minutes	• Disruption Id • Status code • Stats • Category • Severity • Start time • End time • Location (narrative) • X co-ordinate • Y co-ordinate • Origin • Comments	As specified
Tram Stops	X, Y co-ordinates	CentreComm	TfL - CDR	Must	Semi-annual	Name	

Transport for London

Data Type	GIS coding	Displayed by	Data Source	MoSCoW	Min refresh freq.	Hover / quick click display	Full data
Urban Traffic Control	X, Y co-ordinates	CentreComm	TfL – CDR	Must	Weekly	As ful data	• Site • SCOOT Node • Cell • Group / Region • Control status (CSTS) • Weekly auto timetable status • UTC Cycle time Link to live Site Fault Management info for asset
Variable Message System	X, Y co-ordinates	CentreComm	TfL – CDR	Must	Weekly	As full data	• Site No • VMS Type • Description • Status • Location (text) • Status flags • Bus routes • Link to live Site Fault Management info for asset

Transport for London

End of Document

SCHEDULE

5 Project Plan

REDACTED

SCHEDULE 6

Acceptance Testing

1. For the avoidance of doubt, the provisions of this **Schedule 6** shall apply but

   shall be subject to any specific acceptance provisions as may be agreed in

   writing by the parties in addition or by way of amendment.

1.1 The Software (**"Test Items"**) shall be subject to and shall be required to

   satisfy the Acceptance Tests, to demonstrate that they comply with the

   Acceptance Criteria (together with the other requirements of this Agreement)

   before being accepted by the Authority.

1.2 Specific Provisions

   1.2.1 Supplier Software Tests

   The following is intended to allow any software or onsite configuration

   to be delivered in increments (if agreed between the parties) in which

   case the following will apply independently to each increment:

   On or before the date specified within the Project Plan, the Service Provider
   will produce a Test Strategy, Level Test Plans, and Test Specifications
   detailing the set of tests which will be carried out for a given Test Level. It is
   expected that these documents define the scope and how the supplier intends
   to ensure that the configured Software performs in accordance with the
   Specification. These documents will be prepared by the Service Provider and
   agreed by the Authority and will include:

   • List of key functionality;

• Description of the test steps;

• Pass/fail criteria including the results expected to be achieved by

processing such data (**"Acceptance Criteria"**);

• Software Configuration;

• Regression Testing;

• Issue resolution method and timescales; and

• Issue prioritisation.

Supplier test progress for a given Test Level will be reported in Test

Progress Reports at a frequency and format agreed with the Authority. On completion of a given Test Level, a Test Summary Report will be submitted in an agreed format to the Authority at a date defined in the Project Test plan for approval. Where it has been agreed that the Software is delivered in an

incremental manner, there will be Integration Testing carried out to

prove that the combination of increments performs in accordance

with the Specification.

1.2.2 Hardware Acceptance Tests

Unless the Authority require specific tests to be performed in relation to the Hardware, the Service Provider shall perform its own tests to ensure that the Authority's Hardware performs in accordance with its documentation in good time in order to allow the Service Provider to be able to provide the System on time in accordance with the Project Plan. The Service Provider shall provide the Authority with written evidence that the tests have been performed and passed successfully in relation to such Hardware. **The evidence shall**

include a description of the tests undertaken (including details of any automated tools used in the test process) and a full set of test results captured in a Test Summary Report which demonstrates that the hardware provided is fit for purpose to support the software to perform in accordance with the Specification.

1.2.3 Supplier System Tests

On or before the date specified in the Project Plan, the Service Provider will produce a Test Strategy, Level Test Plans and Test Specifications designed to prove that the System/combination of Hardware and Software performs in accordance with the Specification. These will be prepared by the Service Provider and agreed by the Authority and will, at the Authority's option, include:

- Performance Testing;

- Functional Testing;

- Non Functional Testing;

- Reliability Resting;

- Volume Testing;

- Stress Testing;

- Load Testing;

- Failover Testing;

- Regression Testing; and

- Component Integration Testing (where applicable).

Supplier test progress for a given Test Level will be reported in Test

Progress Reports at a frequency and format agreed with the

Authority. On completion of a given Test Level, a Test Summary

Report will be submitted in an agreed format to the Authority at a

date defined in the Project Test plan for approval.

1.2.4 Acceptance Testing

On or before the date specified in the Project Plan, for each software and configuration release, the Service Provider and the Authority will agree a set of Acceptance Criteria and associated Test Specifications. This is to demonstrate to the Authority that each software and configuration release:

- is in accordance with the design documents and the relevant Test Specification;
- is consistent with the agreed Change Request;
- is consistent with the Service Levels;
- is implemented in accordance with good industry practice;
- Issue resolution method and timescales; and
- Issue prioritisation.

These tests will be prepared by the Service Provider and agreed by the Authority and will, include:

- Functional Testing;
- Non Functional Testing; and
- Usability testing.

For Acceptance Testing to proceed, the Supplier must have received sign off of Test Summary Reports for Supplier Software Testing, Supplier Hardware Testing, Supplier System testing and where appropriate Supplier Integration Testing from the Authority.

1.2.5 Test Witnessing

Following Authority's reasonable instructions, at its sole discretion,

may require its employees, agents or sub-contractors to carry out

Test Witnessing, including without limitation:

• Witnessing the Service Provider test planning activities

• Witnessing the execution of the Testing being carried out by the

Service Provider;

• Demonstrating to the Authority's reasonable satisfaction that

adequate modifications and Testing have been performed

leading to closure of any Incidents or Defects associated with the

Test or the successful completion of the Test;

• Witnessing a solution demonstration; and

• Testing by an Authority nominated Third Party, in conjunction

with the Service Provider's Testing.

In relation to all Test Witnessing, the Service Provider shall provide

such access, facilities, Information, Data, explanation, Documentation and
assistance to the Authority and any Third Party nominated by the Authority in
order for the Authority (and/or that Third Party) to prepare for and participate in
such Test Witnessing as the Authority may require, which shall include but
shall not be limited to providing the Authority with the facilities necessary to
witness and evaluate the Testing, including, as a minimum:

• desks;

• telephones;

• modems;

• external network access (with appropriate security, such as via a

virtual private network);

• relevant Hardware; and

• relevant Software.

1.2.6 In the case of all testing set out in this **Schedule 6**, and save where

otherwise agreed by the parties in the relevant Project Plan, the Service Provider shall give the Authority as much notice as possible when the relevant part of the Test Item is ready for testing and, unless the Authority request that the Service Provider perform the tests, the Authority shall give the Service Provider notice in accordance with the Project Plan of the days on which the tests shall be performed by the Authority. The Service Provider shall attend such tests in accordance with this **Schedule 6**.

1.2.7   In the case of any tests and other detail and documentation that is to be agreed under this **Schedule 6**:

1.2.7.1 The parties shall meet together in user groups to discuss the tests, the expected results, the documentation, the testing to be carried out in relation to each and every element of the testing and any other detail that is to be agreed in accordance with this **Schedule 6** as well as the Acceptance Criteria (together the **"Test Specifications"**); And

1.2.7.2 The Service Provider shall be afforded, in each and every case, the opportunity to comment on the suitability of the Test Procedures and the Service Provider shall incorporate all reasonable comments into such Test Procedures and pass those to the Authority for further comment and agreement. Should the parties be unable to agree any of the Test Procedures from time to time, the parties shall escalate the matter in accordance with the

dispute resolution procedure set out in **clause 38.**

    1.2.8 The Service Provider shall formally document each set of Acceptance Tests and the results thereof.

1.3   The Authority shall sign an Acceptance Certificate promptly following successful completion of the Acceptance Tests for the Test Items defined in 1.2.4. Such Acceptance Certificate shall not be of any effect unless signed by the Authority's Service Manager. The Authority shall have no obligation to sign an Acceptance Certificate in relation to any relevant Acceptance Tests unless the Service Provider can demonstrate that the Acceptance Tests have been carried out in accordance with the agreed procedure and the results of the Acceptance Tests objectively demonstrate that all of the Acceptance Criteria have been met. The Authority shall act reasonably in this regard.

1.4   If any of the Test Items fails to successfully pass and satisfy all Acceptance Tests applicable to it, the Authority shall (if the Service Provider is not specified as being responsible for carrying out the Acceptance Tests) notify the Service Provider in writing (**"Failure Notice"**) setting out (where possible) in reasonable detail the suspected nature of the defects giving rise to such failure or failures. In the event the Service Provider receives a Failure Notice or in the event the Service Provider has performed the Acceptance Tests itself unsuccessfully then the Service Provider shall (at its own expense) use its best endeavours to adapt, modify and/or otherwise correct the relevant Test Items to which the Failure Notice relates or, where there is no Failure Notice, the Test Items that have previously failed, in both cases to the extent necessary for those Test Items to comply with the

applicable Acceptance Criteria and resubmit the relevant Test Items for further Acceptance Tests (**"Re-Tests"**) within (or, at the latest, by the expiry of) a correction period reasonably specified by the Authority provided that if any Test Items shall not have passed the applicable Acceptance Tests by any completion date set out in the Project Plan for those items (or such further period of time as the Service Provider and the Authority shall agree in writing), the Authority shall be entitled (in its discretion and without prejudice to its other rights under this Agreement):

1.4.1 to grant further periods of time during which the Service Provider shall be required to adapt, modify and/or otherwise correct the relevant Test Items to which the Failure Notice relates to the extent necessary for that Test Items to comply with the applicable Acceptance Criteria and thereafter re-submit the relevant Test Items for further Re-Tests; or

1.4.2 to sign an Acceptance Certificate accepting such Test Items and agree with the Service Provider a list of exceptions to be attached to the Acceptance Certificate which the Service Provider shall then rectify within the timescales set out in the list or if none are set out then within a reasonable time and should the Service Provider fail to ensure that such exceptions are remedied within such timescale(s) the Authority shall be entitled to exercise (in its discretion) the rights set out in paragraph 1.4.3 or paragraph 1.4.4 or paragraph 1.4.5; or

1.4.3 to sign an Acceptance Certificate accepting the Test Items under the Agreement for all purposes under the Agreement subject to an

agreed refund in respect of the fees (including any fees in respect of the Services paid and/or payable) in respect of the failing Test Items) or (where such fees cannot reasonably be calculated) subject to an adjustment downwards to the overall fees paid and/or payable under the Agreement to fairly reflect the extent to which the Test Items to be provided or performed (as applicable) in accordance with the Agreement (operating as a whole) is impaired by the failure of the relevant Test Items, such adjustment to be agreed between the parties (both acting fairly and reasonably). In default of such agreement, the Authority be entitled to exercise the rights set out at paragraph 1.4.4 or elsewhere in this paragraph 1; or

1.4.4   to reject the Test Items (meaning any or all of them) and serve notice on the Service Provider immediately terminating the Agreement without liability to the Service Provider including any liability to pay any outstanding fees which, at the time of (and but for) such termination, remain outstanding and following giving the Service Provider a right to remedy/rectify at least once in accordance with either paragraph 1.4.1 or 1.4.2, the Authority shall be entitled (in its discretion and without prejudice to its other rights under this Agreement). In the event of any termination pursuant to this paragraph 1.4.4, the Service Provider shall (within fourteen (14) days of the date of such termination) repay to the Authority all fees paid to the Service Provider under the terminated Agreement; or

1.4.5   to (i) itself complete the supply of the Software and Test Items, or to enter into a contract with a third party to effect such completion; and

(ii) the Service Provider shall pay to the Authority the amount by which the reasonable cost to the Authority of completion of the Software and/or Services pursuant to this paragraph 1.4.5 exceeds the agreed fees, and the Authority may deduct the said amount from such amounts (if any) as are due to the Service Provider or to recover such amount as a debt due from the Service Provider; and

(iii) the Authority shall be entitled to use or have used on its behalf all know-how and Intellectual Property Rights owned or controlled by the Service Provider used in or in connection with the Software and/or Services free of charge for the purposes of completion in accordance with this paragraph 1.4.5 and use, amendment, modification and/or enhancement of the Software as envisaged by this Agreement after such completion.

1.5   The Service Provider shall ensure that any corrections made as a result of any failure to pass an Acceptance Test or to be approved in accordance with paragraph 1 shall not adversely impact on any previously successful Acceptance Test or (as applicable) approval procedure in respect of any other Test Item or deliverable(s) or Service(s) (as the case may be). To the extent that any such adverse impacts occur, the Service Provider shall be liable to the Authority in respect of the Authority's reasonable costs in conducting Re-Tests or (as applicable) re-running the relevant approval procedure.

1.6   Any dispute as to whether any Acceptance Test has been passed or whether any failure to provide approval is reasonable in the circumstances shall be referred for resolution in accordance with **clause 38**.

1.7   Acceptance of the Software shall not relieve the Service Provider from

        performing its other obligations under this Agreement and shall not limit the

        warranties provided by the Service Provider under **clause 9.**

SCHEDULE 7

Change Control Procedures

1. **Principles**

1.1 Where the Authority or the Service Provider sees a need to change any of the Services (which includes for the purposes of this **Schedule 7** any aspects of the Software), the TfL Group's Service Manager may at any time request, and the Service Provider's Service Manager may at any time recommend, such amendment only in accordance with the formal Change Control Procedure (**"CCP"**) as set out at paragraph 2 below**.**

1.2 Neither party shall unreasonably withhold its agreement to any amendment (which includes not recommending changes to any Services which are not reasonably necessary) and the Service Provider agrees that it shall not unreasonably withhold its agreement to amend the Specification in order to provide alternative functionality that the Authority may require from time to time. Amendments could include, but shall not be limited to, providing alternative functionality in place of functionality that the Authority identifies they no longer have a requirement for. The price of implementing alternative functionality would be offset against any costs savings made by not implementing the functionality originally required.

1.3 Until such time as an amendment to the Services is made in accordance with this Change Control Procedure, the Authority and the Service Provider shall, unless otherwise agreed in writing, continue to perform the Services in compliance with its terms prior to such amendment.

1.4 Any discussions which may take place between the Authority and the Service Provider in connection with a request or recommendation before the authorisation of a resultant amendment to the Services shall be without prejudice to the rights of either party.

1.5   Any work undertaken by the Service Provider which has not been otherwise agreed in accordance with the provisions of this **Schedule 7** shall be undertaken entirely at the expense and liability of the Service Provider.

Procedures

1.6   Discussion between the Authority and the Service Provider concerning an amendment to the Services shall result in any one of the following:

    1.6.1   no further action being taken;

    1.6.2   a request to amend the Services by the Authority; or

    1.6.3   a recommendation to amend the Services by the Service Provider.

1.7   Where a written request for an amendment is received from the Authority, the Service Provider shall, unless otherwise agreed, submit two (2) copies of a Change Control Note (**"CCN"**) signed by the Service Provider to the Authority within seven days of the date of the request or such other period as the Service Managers shall agree (acting reasonably).

1.8   A recommendation to amend by the Service Provider shall be submitted direct to the Authority in the form of two (2) copies of a CCN signed by the Service Provider at the time of such recommendation and the Authority shall give its response within fourteen (14) days or such other period as the Service Managers shall agree (acting reasonably).

1.9   Each CCN shall contain:

    1.9.1   the title of the amendment;

    1.9.2   the originator and date of the request or recommendation for the amendment;

    1.9.3   the reason for the amendment;

    1.9.4   full details of the amendment including any specifications;

    1.9.5   the price, if any, of the amendment;

1.9.6 a timetable for implementation together with any proposals for acceptance of the amendment;

1.9.7 a schedule of payments, if appropriate;

1.9.8 details of the likely impact, if any, of the amendment on other aspects of the Services including to:

the timetable for the provision of the amendment;

the personnel to be provided;

the amended charges payable under the Services (as now amended);

the Documentation to be provided;

the training to be provided;

working arrangements; and

other contractual issues;

1.9.9 the date of expiry of validity of the CCN; and

1.9.10 provision for signature by the Authority and by the Service Provider.

1.10 For each CCN submitted the Authority shall, within the period of the validity of the CCN:

1.10.1 allocate a sequential number to the CCN; and

1.10.2 evaluate the CCN and, as appropriate:

request further information, or

arrange for two (2) copies of the CCN to be signed by or on behalf of the Authority and return one of the copies to the Service Provider; or

notify the Service Provider of the rejection of the CCN.

1.11   A CCN signed by the Authority and by the Service Provider shall constitute an amendment to the Services and to the Agreement and otherwise no amendment shall have been agreed.

Change Control Note

Change Request No ....

Agreement No…………dated………….

Title of Amendment…………………………..

Originator…………………………………..

The following change is requested to the Agreement identified above

Change Request
(to be completed by the Authority)

Description of Change:

Reason/Justification:

Affected Area(s):

Price:

Timetable for implementation:

Schedule of Payments:

Details of likely impact, if any, of the amendment on other aspects of the Services-

- the timetable for the provision of the amendment;

- the personnel to be provided;

- the amended charges payable under the Services (as now amended);

- the Documentation to be provided

- the training to be provided;

- working arrangements;

- other contractual issues.

I request that the described change be considered for inclusion in the Agreement

Signature ....   Date ..../........./........

Approved by the Authority:

Signature ....   Date ..../........./........

SCHEDULE 8

Security Policies

1. Information Security Policy

2. Information Systems Security Policy

Transport for London

Information Security Policy

Issue date: 16 December 2009

Effective: 1 January 2010

This supersedes any previous policy.

Purpose

1.   The objective of this policy is to ensure that all the Information Transport for London (TfL) holds in order to deliver its services and operations is managed with appropriate regard for Information Security, so as to:

   (a)   Protect its integrity, availability, and confidentiality;

   (b)   Minimise the potential consequences of information security breaches by preventing their occurrence in the first instance, or where necessary, containing and reducing their impact; and

   (c)   Ensure that personal data is afforded the protection required by the Data Protection Act 1998.

2.   This policy applies to all Information held by TfL in any form or medium, electronic, paper or otherwise, including all data held on, or processed by, TfL systems.

3.   External service providers must adhere to the principles of this policy; compliance will be monitored through contractual arrangements and audits.

Definitions

4.   Information: any information, data or records, irrespective of format, which are generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.

5.   Information Governance: a business unit within General Counsel.

6.   Information Management (IM): a business unit within Finance.

7.   Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.

8.   Information Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of Information within the TfL Group.

MAYOR OF LONDON

9.   Information Security: the ability to protect the integrity, availability, and confidentiality of Information held by TfL and to protect Information from unauthorised use, modification, accidental or intentional damage or destruction.

10.   Information Security Breach: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.

11.   Information Security Incident: a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening information security.

12.   Information System: Information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.

13.   Internal Audit: a business unit within General Counsel.

14.   TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.

14.   Transport for London (TfL): the statutory corporation and its operating subsidiaries.

Organisational scope

15.   This policy applies to TfL and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for TfL.

Policy statement

14.   TfL depends on Information and Information Systems to support and develop its key business objectives, including the provision of public transport services and the implementation of the Mayor of London's Transport Strategy. TfL will adopt appropriate technical and organisational arrangements in accordance with this policy to protect the resilience, integrity, availability and confidentiality of the Information it holds (including personal data relating to both customers and employees) and the systems in which the Information resides.

15.   This policy has been developed with reference to the following best practice standards and guidance:

        (a)   Information Security Standard ISO/IEC 27001 and associated Code of Practice for Information Security ISO/IEC 27002:2005.

        (b)   Her Majesty's Government (HMG) Security Policy Framework.

        (c)   Cross Government Mandatory Minimum Measures for Data Handling.

        (d)   Government Protective Marking Scheme (GPMS).

        (e)   Payment Card Industry Data Security Standard (PCI DSS).

Policy content

16.   TfL's policy is to ensure that:

(a)   Information Security is considered as a fundamental and integral part of all TfL operations.

(b)   Statutory requirements to safeguard the security of Information are met and the accuracy, completeness and segregation of personal data are assured.

(c)   Information is accessible to authorised users when they need it and is assigned an appropriate security classification.

(d)   ICT systems, networks and other key infrastructure components are protected from harm and the integrity of Information is maintained and protected from attack and unauthorised access or alteration.

(e)   Information Risk will be considered and afforded a priority in decisions within TfL in the same way as financial and operational risk. This will be reflected in corporate and local risk registers. Information Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect TfL's information or information systems.

(f)   Business continuity plans, including disaster recovery plans, are implemented to support business needs and appropriate Information Security training is given to TfL Personnel.

(g)   All Information Security Breaches, actual or suspected, are reported and investigated and a culture exists where improving Information Security procedures is encouraged.

(h)   All necessary measures are taken in order to comply with the Payment Card Industry Data Security Standards (PCI DSS), which are mandatory for organisations processing payment card transactions.

Responsibility for Information Security

17.   Each TfL employee is responsible for actively supporting this policy and must ensure that their use of TfL's Information or Information Systems is in accordance with it. Employees must seek advice in the event of uncertainty in relation to this issue.

18.   All Cost Centre and Project managers are directly responsible for the security of Information within their business areas.

19.   Information Owners are responsible for ensuring that TfL Personnel within their area of control are aware of this policy and are adequately trained in Information Security.

20.   Information Owners are responsible for the assessment and reporting of Information Risk within each business unit.

21.   Information Owners will define and document relevant statutory and contractual requirements for Information Systems.

22. Information Owners will implement appropriate procedures to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights including copyright, design rights and trademarks.

23. Information Owners, with support from TfL Personnel who lead on business continuity planning within the relevant business area, will manage and co-ordinate strategies for resilience, including business recovery following information loss or corruption or unauthorised disclosure or access.

24. TfL Personnel who lead on business continuity planning within their business area are responsible for co-ordinating the creation and maintenance of business continuity plans for all departments across TfL, which take account of the requirements of this policy where appropriate.

25. Information Governance, Internal Audit and IM are responsible for managing actual or suspected Information Security Incidents and Breaches and recommending additional or improved security measures to prevent their reoccurrence.

26. Information Governance is responsible for the interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.

27. IM are responsible for advising the business on the technical measures required to implement this policy and for their implementation on TfL's Information Systems and for ensuring that appropriate technical measures are in place to protect the security of electronic Information.

Procedures/Guidelines/Processes

28. All Information held by TfL must be managed in accordance with TfL's Privacy and Data Protection Policy, Information and Records Management Policy and Information Access Policy.

29. Appropriate Information Security procedures and TfL Standards will be implemented in support of this policy. These will include Standards and procedures as listed in the Annex to this Policy.

30. TfL will have in place an Information Security Classification Standard for protectively marking Information. Security classifications will be applied to all of TfL's Information on creation or receipt, irrespective of format or medium, and Information classified according to this Standard must be transmitted, stored and disposed of as required by the classification Standard and its accompanying instructions.

31. TfL personnel handling Information which has been protectively marked in accordance with HMG's Security Policy Framework (SPF) will adhere to the requirements of the SPF.

32. Actual or suspected Information Security Incidents involving personal or sensitive personal data (as defined by the Data Protection Act 1998) must be reported to Information Governance in order for the incident to be managed in accordance with the Incident Management Procedure for the Loss or Unauthorised Disclosure of Personal Data.

33.   Internal Audit will perform a periodic audit of the security processes, procedures and practices of TfL and its service providers to monitor compliance with this policy.

Approval and amendments

34.   This policy was approved by the Commissioner on 18 November 2009.

35.   This policy was approved by the Audit Committee on 16 December 2009.

36.   Following an organisational restructure, a number of minor amendments to this Policy were made on 2 May 2012.

37.   This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

38.   TfL's General Counsel is the designated owner of this policy.

Annex: Information Security Standards and procedures

Standards and procedures covering the following topics will be implemented in support of the Information Security Policy:

- Physical security of data centres, communications rooms and sensitive zones.
- Incident management.
- Business continuity.
- CMDB (IT asset register).
- Security vetting for sensitive roles within Information Management (IM).
- IT user registration.
- Back-up.
- Cryptographic controls.
- Third party connections.
- Change management.
- Development and test areas.
- Access controls.
- System requirements analysis.
- Mobile computing and remote working.
- Input data validation.
- Integrity of software and information.
- Acceptable use and user responsibilities.
- Information handling.

Transport for London

Information Systems Security Policy

Issue date: 19 October 2010
Effective: 19 October 2010

This supersedes any previous policy.

Purpose

1. TfL is critically dependent on both its information and information systems in achieving its strategic vision. If confidential TfL information were disclosed to unauthorised persons, become unavailable or unreliable, the company could suffer serious financial, commercial or legal damage.

2. The purpose of this information systems security policy is to make sure that information held on or processed by TfL's information systems is secured commensurate with the requirements stipulated within the TfL's Information Security Policy. In particular, it will ensure that all information held or processed on TfL's information systems is protected from harm and unauthorised access; is correct and accurate and is available when needed.

Definitions

3. **IS Security Framework** is made up of the TfL Information Security policy, this policy and a number of IM Security principles, functional policies, standards, and guidelines. The framework is published in the Your IM Controlled Documents Library.

4. **Information assets**: any information, data or records, irrespective of format, which are generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.

TfL UNCLASSIFIED

Transport for London

5. **Information owners**: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.

6. **Information Security**: the ability to protect the integrity, availability, and confidentiality of information held by TfL and to protect information from unauthorised use, modification, accidental or intentional damage or destruction.

7. **Information Security Breach**: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.

8. **Information Security Incident**: a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

9. **Information System**: information in all electronic media, hardware, software and supporting networks (excluding SCADA systems) and the processes and human resources that support its acquisition, storage and communication.

10 **SCADA systems**: Supervisory Control and Data Acquisition Systems includes operational control and signalling systems and building services control systems.

11 **TfL Personnel**: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.

12 **Transport for London (TfL)**: the statutory corporation and its operating subsidiaries.

TfL UNCLASSIFIED

Transport for London

Organisational scope

13 This policy applies to TfL and to commercial organisations or service providers (including agencies or consultancy companies) contracted to operate or supply information systems or services to TfL.

14 The policy applies to all users of TfL Information Systems.

Policy statement

15 information systems will be operated in a secure manner in accordance with TfL's Information Security Policy.

16 This policy and supporting principles, functional policies, standards and guidelines constituting the IS Security Framework, as shown in Appendix 1, will be formally published and made available to all users of TfL information systems.

17 The IS security framework has been developed with reference to the following best practice standards and guidance:

    17.1   Information Security Standard ISO/IEC 27001 and associated Code of Practice for Information Security ISO/IEC 27002:2005.

    17.2   Her Majesty's Government (HMG) Security Policy Framework.

    17.3   Payment Card Industry Data Security Standard (PCI DSS).

Policy content

18 The Information Systems Security Policy is to ensure that:

    18.1   information systems, services and TfL personnel involved in their use, operation and support comply with the IS Security Framework

TfL UNCLASSIFIED

Status: Approved   IS Security Policy Version: 1.0

Transport for London

18.2   information assets are protected against unauthorised access
        and change

18.3   information assets are accessible to authorised users when they
        need it

18.4   information assets are clearly marked with a security
        classification, in accordance with TfL's Information Security
        Classification

18.5   information assets are protected and handled in accordance with
        the requirements of their security classification

18.6   information assets will be managed in accordance with TfL's
        Privacy and Data Protection Policy, Information and Records
        Management Policy and Information Access Policy.

18.7   information systems, networks and other key infrastructure
        components are protected from harm, in line with formal risk
        assessment and risk acceptance models

18.8   information systems, networks and other key infrastructure
        components are subjected to security testing.

18.9   TfL complies with all relevant regulatory, contractual and
        legislative requirements

18.10   information Systems Disaster Recovery Plans are produced,
        maintained and regularly tested in support of Business
        Continuity Plans developed by the Business Continuity
        Managers

18.11   information systems security awareness is made available to all
        TfL personnel

TfL UNCLASSIFIED

Status: Approved   IS Security Policy Version: 1.0

Transport for London

18.12   all information systems security incidents or beaches, actual or suspected, are investigated

18.13   information systems security processes, procedures and practices are documented and reviewed regularly and, where necessary, are updated to ensure continued relevance and compliance with this policy

19   Deliberate breach of or failure to comply with this policy will result in disciplinary action in accordance with HR Discipline at Work Policy

Implementation

20. This policy will apply to all new IM systems and projects with immediate effect.

21. Existing IM Systems and projects may not be compliant with this policy.

Responsibility for Information Systems Security

22   The Chief Information Officer (Your IM)

22.1   will be responsible for assuring compliance with this Policy of all information systems operated for or behalf of TfL, but excluding SCADA control systems.

22.2   will chair an Information Systems Security Forum to ensure that there is clear direction and visible management commitment to information systems security within TfL. Membership of the Forum will include the Director of Information Management (LU); the Heads of Business Directorates with departments responsible for the operation or provision of IM services outside of Your IM (as listed in Appendix 2) and the Department Heads of Your IM

TfL UNCLASSIFIED

Status: Approved   IS Security Policy Version: 1.0

Transport for London

22.3 will review of this policy to ensure that it remains valid and fit for purpose. Such review will be undertaken at least annually or earlier if changes in IM governance or organisation require it.

23 The Director of Information Management for London Underground; Heads of TfL Business Directorates with departments responsible for the operation or provision of IM services in their business areas (as listed in Appendix 2), and the Department Heads of Your IM are responsible for assuring:

23.1 the development, enforcement, management and maintenance of information systems security, and shall deploy the necessary controls to demonstrate compliance of information owners, custodians and users to the IT Security Framework;

23.2 that agencies and third parties with which they are engaged contractually to provide information or information services, within the framework of these contracts, also comply with this policy;

23.3 the appropriate designation of responsibilities for the management and documentation of information systems security, processes and procedures within the business in compliance with this policy;

23.4 the oversight of their respective information systems security posture and will ensure that the business is in compliance with this policy;

23.5 all TfL personnel in their business area are made aware of their responsibility for the security of TfL information systems and the information stored or processed on them and they use TfL information systems in accordance with HR Electronic Communications (including Email and Internet) and Equipment Usage Policy.

TfL UNCLASSIFIED

Status: Approved   IS Security Policy Version: 1.0

Transport for London

23.6   the development and maintenance of appropriate measures of compliance with this Policy to be reported every 3 months to the Information Systems Security Forum.

24 Your IM

24.1   will develop information systems security principles, standards and guidelines to support this policy (known as the IT Security Framework) which will be published and made available to all TfL personnel;

24.2   will develop and maintain information systems security awareness training materials for the use of all TfL personnel

25 All personnel whether as IM staff, Information Owners or as users of TfL information systems are responsible for:

25.1   actively supporting this policy

25.2   using TfL's information systems in a responsible and secure manner

25.3   reporting actual or suspected information systems security incidents to the IM security service

26 TfL Internal Audit will audit the information systems security processes, procedures and practices of TfL and its service providers to provide assurance to the Audit Committee that information systems security risks are being managed effectively and in accordance with TfL's policies.

Review

27.1   This policy will be subject to annual review.

27.2   The date of next review is 19/10/2011

TfL UNCLASSIFIED

Transport for London

Approval and amendments

28   Policy Liaison Group consultation on this policy was completed on 11/06/2010

29   This policy was approved by the IM Leadership Team on19/10/2010.

30   This policy will be subject to annual review or as considered appropriate by Your IM Chief Information Officer.

Policy owner

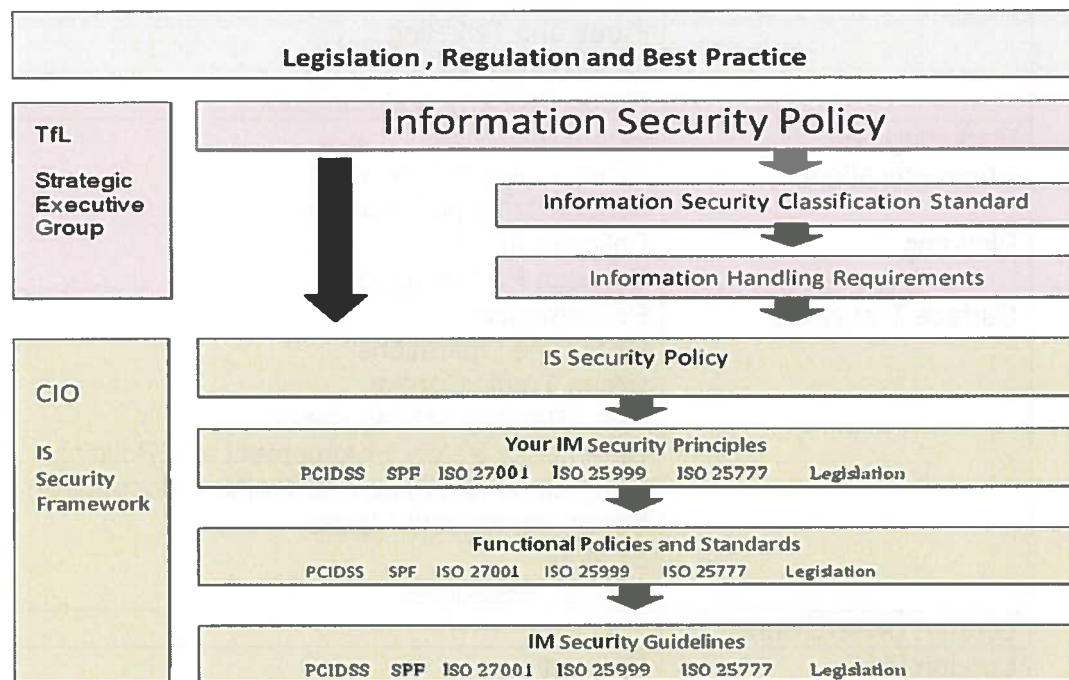Your IM Chief Information Officer is the designated owner of this policy.

Status: Approved   IS Security Policy Version: 1.0

Transport for London

Appendix 1 IS Security Framework

Legislation , Regulation and Best Practice		
TfL Strategic Executive Group	**Information Security Policy**	
	Information Security Classification Standard	
	Information Handling Requirements	
CIO IS Security Framework	IS Security Policy	
	Your IM Security Principles PCIDSS SPF ISO 27001 ISO 25999 ISO 25777 Legislation	
	Functional Policies and Standards PCIDSS SPF ISO 27001 ISO 25999 ISO 25777 Legislation	
	IM Security Guidelines PCIDSS SPF ISO 27001 ISO 25999 ISO 25777 Legislation	

TfL UNCLASSIFIED

Page 9 of 10

Status: Approved   IS Security Policy Version: 1.0

Transport for London

Appendix 2 - TfL Business Directorates with Departments responsible for the operation or provision of IM services

Business Directorate	Department
Finance	Corporate Finance Fares and Ticketing Group Procurement Group Property and Facilities
Marketing and Communications	Group Marketing Group Customer Services London Transport Museum
Planning	Policy Analysis Borough Partnerships
Surface Transport	Performance Real Time Operations Urban Traffic Control Road Network Management Community Safety Enforcement and Policing Congestion Charging and Traffic Enforcement Better Routes and Places Strategy Human Resources
London Underground	
London Rail	Crossrail Overground

TfL UNCLASSIFIED

Status: Approved   IS Security Policy Version: 1.0

SCHEDULE 9

Agreed Equality Policy

Not used

SCHEDULE 10

Exit Management

2. Definitions

In this Schedule, the following expressions shall have the following meanings unless inconsistent with the context:

"Authority 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 Service Provider by or on behalf of the Authority; or (ii) which the Service Provider is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Data Controller.
"Authority Furnished Items"	means any items issued or otherwise furnished in connection with this Agreement by or on behalf of the Authority.
"Data Controller"	has the same meaning as set out in the Data Protection Act 1998.
"Personal Data"	has the meaning given to it by section 1(1) in the Data Protection

Act 1998.

"Replacement Service Provider"	means any replacement supplier or provider to the Authority of the Agreement (or any part of it)

2.   **Overview**

2.1   Service Provider is required to ensure the orderly transition of the Services from the Service Provider to the Authority and/or any Replacement Service Provider in the event of termination (including partial termination) or expiry of this Agreement. This Schedule sets out the principles of the exit and service transfer arrangements that are intended to achieve such orderly transition and which shall form the basis of the Exit Plan. For the avoidance of doubt and unless the Authority requires otherwise in writing, the Service Provider shall be responsible for the overall management of the exit and service transfer arrangements in accordance with this Schedule and the Exit Plan.

2.2   Where required by the Authority, no later than the Milestone for completion of user acceptance testing, and thereafter as agreed, the Service Provider shall prepare an Exit Plan for review by the Authority. The Authority shall review the Exit Plan within twenty (20) working days of receipt from the Service Provider and shall notify the Service Provider of any suggested revisions to the Exit Plan. In this respect, the Authority will act neither unreasonably, capriciously nor vexatiously. Such suggested revisions shall be discussed and the parties shall use reasonable endeavours to resolve such revisions within ten (10) working days. The agreed Exit Plan shall be signed as approved by each party. If the parties are unable to agree the contents of the revised Exit Plan then such dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3.

3.1   The Exit Plan shall provide comprehensive proposals for the activities and the associated liaison and assistance that will be required for the successful transfer of the Services, including the following details:

2.2.1. proposals for the identification and transfer of documentation providing details of the Software and Services;

2.2.2. proposals for the identification of all Software and Services;

2.2.3. proposals for the identification of all maintenance agreements and support agreements utilised by the Service Provider in connection with the provision of the Services, together with details of the relevant lessors and contractors, the payment terms, expiry dates and any relevant novation and/or early termination provisions;

2.2.4. proposals for the identification and return of all Authority Furnished Items in the possession and/or control of the Service Provider or any third party (including any Sub-Contractor);

2.2.5. a detailed summary identifying the owners of title and risk in the Software and Services and Authority Furnished Items following transfer of the Services;

2.2.6. proposals to enable the Authority or the Replacement Service Provider to recruit suitably skilled personnel;

2.2.7. proposals for the training of key members of the Replacement Service Provider's personnel in connection with the continuation of the provision of the Services following the expiry or termination (howsoever arising) of this Agreement charged at rates agreed between the parties at that time;

2.2.8. proposals for the granting of licences to use Software necessary for the Authority's continued receipt of the Services and the provision of copies of all related documentation;

2.2.9. proposals for the transfer of all Authority Data then in the Service Provider's possession to either the Authority or a Replacement Service Provider, including:

2.2.10. an inventory of all Authority Data;

2.2.11. details of the data structures in which the Authority Data is stored, in

the form of an agreed data model together with information on other data structures in which the Authority Data could be stored;

2.2.12.   proposed transfer methods, both physical and electronic; and

2.2.13.   proposed methods for ensuring the integrity of the Authority Data on transfer;

2.2.14.   proposals for providing the Authority or a Replacement Service Provider copies of:

(i)   all documentation used in the provision of the Software and Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the Service Provider or Service Providers sub-contractor; and

(ii)   all documentation relating to the use and operation of the Software

2.2.15.   proposals for the methods of transfer of the Services to the Authority or a Replacement Service Provider;

2.2.16.   proposals for the supply of any other information or assistance reasonably required by the Authority or a Replacement Service Provider in order to effect an orderly hand over of the provision of the Services.

Exit Plan shall be reviewed and updated by the Service Provider. In this regard, the Service Provider shall provide a revised version of the Exit Plan to the Authority in the first month of each contractual year (commencing with the second contract year). The revised Exit Plan shall be reviewed and agreed in accordance with the provisions of   this   Schedule.

SCHEDULE 11

SAFE Software Sub-Licence

REDACTED

SCHEDULE 12

Tender Response to Functional Requirements

REDACTED

SCHEDULE 13

Tender Response to Non-Functional Requirements

REDACTED

SCHEDULE 14

Authority Clarifications from BAFO

REDACTED