

Schedule 11.2 – Risk Management

TfL RESTRICTED

Restricted to: TfL Group, Contractor Group and Consultants with NDA

Copyright Transport for London 2014

Contents

1	Introduction	3
1.1	Scope and Purpose.....	3
1.2	Risk Categories.....	3
1.3	Documents to be Submitted	4
2	Risk Management	5
2.1	Risk Management Plan	5
2.2	Risk Schedule	5
2.3	Review and Updating	6
2.4	Reports and Meetings	7
	Appendix 1 – TTL Risk Scoring	8
	Risks to Project cost and/or Project Plan	8
	Contract Risks	8
	Security Risk.....	10
	RAG Status.....	10

1 Introduction

1.1 Scope and Purpose

- 1.1.1 This Schedule sets out the requirements for the Contractor to prepare a plan setting out the arrangements for identifying, recording, monitoring, mitigating, controlling and assessing Risks throughout the Term.
- 1.1.2 The Contractor shall implement risk management processes consistent with ISO 31000.
- 1.1.3 The objectives of this Schedule are to ensure that:
 - (a) the Contractor implements appropriate risk management processes, taking into account the Risks relating to the Services and/or the IRC System;
 - (b) Risks are identified and managed effectively by the Contractor throughout the Term; and
 - (c) TTL and the Contractor adopt the best approach to managing any shared Risks.
- 1.1.4 The Documents to be submitted pursuant to paragraph 1.3.1 of this Schedule provide Assurance to TTL that the Contractor will manage any known or likely Risks and give sufficient attention to the identification, assessment, control, mitigation and elimination of new Risks (as applicable) such that the Services will be provided in accordance with the Contract.
- 1.1.5 The Documents to be submitted pursuant to paragraph 1.3.1 of this Schedule will also provide visibility of those Risks that are shared with TTL and those requiring an input from TTL, so that TTL and the Contractor may jointly manage these Risks through Variations, VfM Initiatives or agreement with TTL on a case by case basis.

1.2 Risk Categories

- 1.2.1 The Contractor shall ensure that any Risks are grouped under the following categories:
 - (a) "**Project Risks**", meaning all risks associated with individual Projects and Programmes;
 - (b) "**Security Risks**", meaning all risks associated with the security of the IRC System and information security and including any risks identified in the ISMS and/or pursuant to Schedule 9.4 (Security Management); and
 - (c) "**Contract Risks**", meaning all risks associated with the Services and/or the IRC System which are not Project Risks or Security Risks.
- 1.2.2 The Contractor shall ensure that each category of Risk is capable of being reported separately.
- 1.2.3 In addition, the Contractor shall ensure that Project Risks are capable of being reported separately by Project and/or Programme.

1.3 Documents to be Submitted

- 1.3.1 The Contractor shall prepare, submit and maintain throughout the Term the following Documents in accordance with the requirements of this Schedule:
- (a) the Risk Management Plan; and
 - (b) the Risk Schedule.

2 Risk Management

2.1 Risk Management Plan

2.1.1 The Contractor shall ensure that the Risk Management Plan includes the following information as a minimum:

- (a) details of the Contractor's Risk management strategy;
- (b) details of the resources the Contractor proposes to utilise in order to implement the Risk management strategy;
- (c) details of the Contractor's processes for Risk:
 - (i) identification;
 - (ii) recording;
 - (iii) prevention;
 - (iv) analysis;
 - (v) classification;
 - (vi) monitoring;
 - (vii) mitigation; and
 - (viii) control; and
- (d) the Risk Schedule in accordance with paragraph 2.2 below.

2.1.2 The Contractor shall provide details of any recognised techniques or software tools that it uses in relation to Risk management.

2.2 Risk Schedule

2.2.1 The Contractor shall ensure that the Risk Management Plan includes a schedule of Risks (the "**Risk Schedule**") which shall record the status and current impact of the identified or likely Risks. The Contractor shall add new Risks to the Risk Schedule promptly as and when they are identified.

2.2.2 The Contractor shall ensure that the Risk Schedule is in tabular format and includes as a minimum for each Risk the following data fields:

- (a) the Risk category in accordance with paragraph 1.2;
- (b) subcategory (e.g. individual Project and/or Programme);
- (c) a unique reference;
- (d) Risk description including details of the cause;
- (e) the Risk status (e.g. "emerging", "open", "closed - fully mitigated", "closed – probability 100% (this has become an issue)");

- (f) the Risk scoring (which shall be compatible with the TTL Risk scoring set out in Appendix 1 for the relevant Risk category);
 - (g) a Risk owner (i.e. the person(s) responsible for dealing with the Risk);
 - (h) the specific part(s) of the Services or the IRC System affected by the Risk item, including Module ID where appropriate;
 - (i) the date when the Risk was identified;
 - (j) the target date when the Risk is anticipated to be resolved;
 - (k) the actual date when the Risk is resolved;
 - (l) the financial component of the impact assessment of the Risk (expressed in pounds sterling (£s));
 - (m) the time component of the impact assessment of the Risk (expressed in days);
 - (n) the probability assessment (i.e. likelihood of the Risk occurring) (expressed as a percentage);
 - (o) overall financial impact (calculated as (l) multiplied by (n));
 - (p) overall time impact (calculated as (m) multiplied by (n));
 - (q) details of mitigation measures for each Risk;
 - (r) the RAG status of the Risk (i.e. Red, Amber or Green) in accordance with Appendix 1 of this Schedule, including a reasonable explanation for such status if the Contractor considers that a different RAG status from those set out in Appendix 1 is appropriate; and
 - (s) identification of whether the Risk is a shared Risk and any TTL dependencies relating to each Risk.
- 2.2.3 The Risk Schedule shall be capable of being sorted by the data fields described in paragraph 2.2.2.
- 2.2.4 The Contractor shall clearly identify in the Risk Schedule the most significant Risks which shall, as a minimum, include those Risks which would be scored as VH or H using the TTL Risk scoring set out in Appendix 1 (each a "**Significant Risk**").
- 2.2.5 The Contractor shall respond to reasonable requests from TTL from time to time to provide sufficient evidence to TTL to justify the entries in the Risk Schedule.

2.3 Review and Updating

- 2.3.1 The first Risk Management Plan and first Risk Schedule shall be provided by the Contractor to TTL on the Service Commencement Date.
- 2.3.2 The Risk Management Plan shall be reviewed, updated and re-issued by the Contractor to TTL at least every six (6) months following the Service Commencement Date.

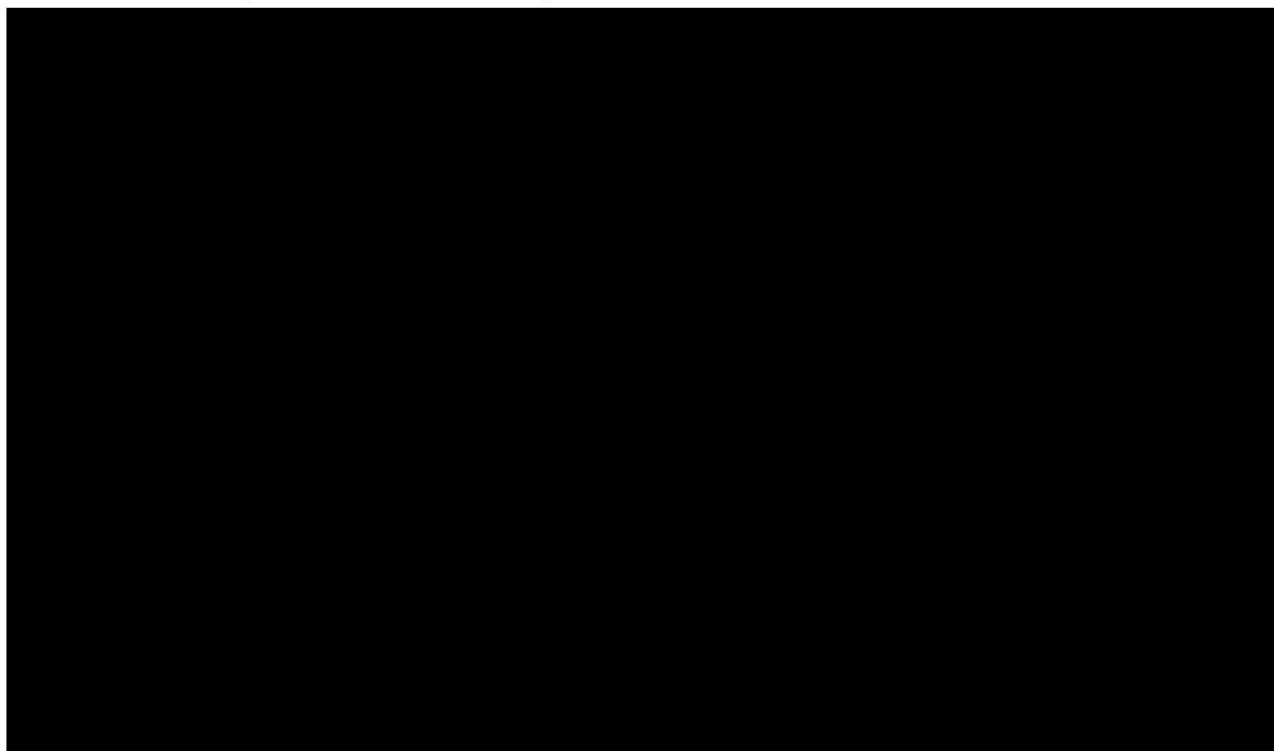
- 2.3.3 The Risk Schedule shall be reviewed and updated by the Contractor at least every Period and a summary copy of the updated Risk Schedule shall be submitted to TTL as required in paragraph 2.4 of this Schedule and on request by TTL. If the Contractor fails to comply with this obligation it shall prepare and issue a Corrective Action Plan in accordance with Schedule 12.4 (Contract Management)
- 2.3.4 The Contractor shall give TTL access to the current issue of the Risk Schedule on request and make available from time to time copies of the Risk Schedule as required by Clause 65 (Records, Audit and Inspection). If the Contractor fails to comply with this obligation it shall prepare and issue a Corrective Action Plan in accordance with Schedule 12.4 (Contract Management)

2.4 Reports and Meetings

- 2.4.1 The Contractor shall provide to TTL a risk status report of Project Risks within each Project Report and Programme Report in accordance with Schedule 10.2 (Programme and Project Lifecycle) and shall include a copy of the Project Risks which are Significant Risks from the Risk Schedule in the Project Report and/or Programme Report in accordance with Schedule 10.2 (Programme and Project Lifecycle) and the actions the Contractor is taking to mitigate or obviate the impact of those Risks. These Significant Risks shall then be discussed at the next Project or Programme Review Meeting.
- 2.4.2 The Contractor shall provide to TTL a risk status report of Security Risks in accordance with Schedule 9.4 (Security Management) which shall include a copy of the Security Risks which are Significant Risks from the Risk Schedule and the actions the Contractor is taking to mitigate or obviate the impact of those Risks. These Significant Risks shall then be discussed at the next Information Security Forum.
- 2.4.3 The Contractor shall provide to TTL a risk status report of Contract Risks within the Service Performance Report in accordance with Schedule 4.1 (Service Delivery), which shall include a copy of the Contract Risks which are Significant Risks from the Risk Schedule and the actions the Contractor is taking to mitigate or obviate the impact of those Risks. These Significant Risks shall then be discussed at the next Service Review Meeting.
- 2.4.4 Where the Contractor considers that a Risk or Risks are shared with TTL, then the Contractor shall notify TTL and TTL shall arrange to meet with the Contractor to discuss the Risks in detail and to discuss and agree the allocation of responsibilities and the means of monitoring and controlling the Risks. These discussions shall be confirmed in writing by TTL following such meeting so that both Parties are clear as to their responsibilities, and the Contractor shall adjust the Risk Schedule accordingly within ten (10) Business Days of TTL's confirmation.
- 2.4.5 Depending on the nature of the shared Risk and its timing, the Contractor shall report on the impact of the Risk in either the Project Report, Programme Report, Programme Portfolio Report, the Service Performance Report or report of Security Risks as determined by TTL, and the Risk shall be discussed at the corresponding review meeting.
- 2.4.6 TTL shall be entitled to call separate meetings from time to time to review the Risk Schedule in detail or to focus on Significant Risks or shared Risk items, and the Contractor shall make available such Contractor Personnel (including relevant Risk owners) as necessary and appropriate to attend such meetings.

Appendix 1 – TTL Risk Scoring

Risks to Project cost and/or Project Plan



If a Project Risk meets the criteria of more than one category of risk scoring in the table above, that Project Risk shall be categorised according to the highest applicable risk scoring.

Contract Risks

Scoring	Customer	Impact on TTL Group's Reputation
VH	Any one of the following: <ul style="list-style-type: none">• Suspension of Customer facing functionality across an entire mode of transport (e.g. bus, river, London Underground) or in relation to an entire category of Card for more than one (1) day• Part suspension of Customer facing functionality across an entire mode of transport (e.g. bus, river, London Underground) or in relation to an entire category of Card for more than one (1) week• Very high impact on functionality which supports Customer facing services (e.g. Customer information)	Risk results in significant ongoing negative media coverage and major loss of confidence/significant intrusion by regulators/stakeholders leading to one or more of the following outcomes: <ul style="list-style-type: none">• Fundamental changes to the operating model/structures• High profile management (e.g. Directors) changes• Fundamental changes to operating and safety procedures
H	Any one of the following: <ul style="list-style-type: none">• Full suspension of Customer facing functionality across an entire mode of transport (e.g. bus, river, London Underground) or in relation to an entire	Risk results in ongoing negative media coverage and loss of confidence/significant intrusion by regulators/stakeholders leading to one of the following outcomes: <ul style="list-style-type: none">• Sustained (i.e. occurring during one (1)

Scoring	Customer	Impact on TTL Group's Reputation
	<p>category of Card for more than four (4) hours</p> <ul style="list-style-type: none"> Part suspension of Customer facing functionality across an entire mode of transport (e.g. bus, river, London Underground) or in relation to an entire category of Card for one (1) day Closure of a Ticket Office Nominated Site or any of the Nominated Stations Highly severe repeated Service impacts (e.g. Customer facing functionality across a mode of transport unavailable or in relation to an entire category of Card more than once in a two (2) week period) High impact on functionality which supports Customer facing services (e.g. Customer service, Customer information) 	<p>or more weeks) diversion of Directors' and senior managers' time, energy and resources away from business as usual activities and planned projects in order to deal with media and/or feedback</p> <ul style="list-style-type: none"> Loss of trust leading to fundamental changes to governance arrangements High impact on operations (e.g. Stations closed)
M	<p>Any one of the following:</p> <ul style="list-style-type: none"> Suspension of validation or retail at an individual Site Repeated suspension of validation or retail at an individual Site Medium impact on functionality which supports Customer facing services (e.g. Customer information) 	<p>Risk results in negative media coverage and loss of confidence/increased intrusion by regulators/stakeholders, leading to one or more of the following outcomes:</p> <ul style="list-style-type: none"> Short-term (i.e. less than one (1) week) diversion of Directors' and senior managers' time, energy and resources away from business as usual activities and planned projects in order to deal with media and/or feedback Sustained (i.e. more than one (1) week) diversion of Directors' and senior managers' time, energy and resources away from business as usual activities and planned projects in order to deal with media and/or feedback Limited impact on operations (e.g. specific Services unavailable)
L	<p>Any one of the following:</p> <ul style="list-style-type: none"> Loss of Key Functionality on any individual Device Repeated loss of Key Functionality on any individual Device Minor impact on functionality which supports Customer facing services (e.g. Customer information) 	<p>Risk results in short-term negative media coverage or impact on relations with regulators/stakeholders leading to one or more of the following outcomes:</p> <ul style="list-style-type: none"> Significant negative feedback from Customers via the TfL customer service centre or from stakeholders via media outlets or sites (e.g. Twitter, blogs, etc.) Short-term (less than one (1) week) diversion of middle managers' time, energy and resources away from business as usual activities and planned projects in order to deal with media and/or feedback
VL (N)	Negligible impact on Services	Risk has negligible impact on regulators/stakeholders but does impact Customers and employees leading to one of

Scoring	Customer	Impact on TTL Group's Reputation
		the following outcomes: <ul style="list-style-type: none">• Low level of negative feedback from Customers via the TfL customer service centre or from stakeholders via media outlets or sites (e.g. Twitter, blogs)

If a Contract Risk meets the criteria of more than one category of risk scoring in the table above, that Contract Risk shall be categorised according to the highest applicable risk scoring.

Security Risk

The Contractor shall, on the Service Commencement Date, prepare and provide to TTL for Assurance a methodology for the categorisation of Security Risks as "Very High (VH)", "High (H)", "Medium (M)", "Low (L)" and "Very Low (VL (N))". The Contractor shall take into account the following principles when preparing such categorisation:

- **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorised changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- **Loss of Availability:** If a mission-critical IT system is unavailable to its end users, the organisation's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organisation's mission.
- **Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorised disclosure. The impact of unauthorised disclosure of Confidential Information can range from the jeopardising of national security to the disclosure of data protected under Data Protection Legislation. Unauthorised, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organisation.

RAG Status

For guidance:

- Risks with a risk scoring of VH or H shall have a Red RAG status
- Risks with a risk scoring of M shall have an Amber RAG Status
- Risks with a risk scoring of L or VL shall have a Green RAG status

The Contractor shall have discretion to categorise Risks with a different risk scoring than above as Red, Amber or Green if it reasonably considers such categorisation appropriate.