

**Date:** 8 March 2016

**Item:** Strategic Risk Management – Update on New Approach and Reporting Documentation

---

**This paper will be considered in public**

## **1 Summary**

The purpose of this paper is to update the Committee with an overview of the work undertaken to date on an improved risk management process; the proposed new approach to TfL Strategic Risk Management and the new design of certain aspects of Strategic Risk reporting documentation.

## **2 Recommendations**

### **2.1 The Committee is asked to:**

- (a) agree that an improvement and change in the overall risk management process is desirable; and**
- (b) review the changes to the Strategic Risk Management approach and reporting documentation.**

## **3 Background**

- 3.1** Over the past quarter we have commenced a review of the risk management process in TfL with special emphasis on Strategic Risk Management. This has been based on reviewing the TfL Risk Management Procedures and related standing documentation. We have also engaged with the Business and Corporate Risk Managers during an interactive workshop session, to discuss the approach to Strategic Risk Management in depth and enable them to offer input on the identified Strategic Risks. Follow up sessions have also been held with senior members of both the Internal and External Audit teams.
- 3.2** The output from this process is an initial evaluation of how the overall TfL risk management activities and systems can be improved, followed by a proposed new approach to Strategic Risk and the presentation of related and refreshed risk reporting documentation.
- 3.3** A Strategic Risk Report was last presented to the Audit and Assurance Committee on 8 October 2015. In this and previous submissions, all Strategic Risks were consolidated into the seven Pan-TfL Risks (for example, TfL 01 Maintaining a Balanced Plan, TfL 02 People Risk). With this method of presentation, some individual Strategic Risks were masked in the larger Pan-TfL categories, diluting attention from real risks.

- 3.4 Risks were previously assessed on a residual basis (after taking existing control activities into account), both quantitatively and qualitatively.
- 3.5 Although the previous approach also provided a “target” assessment, which should be an assessment of the amount of risk that the organisation is willing to take to meet its strategic objectives, the assessment was a future control status – i.e. the status of the risk after improvement actions have been implemented. This is technically incorrect and consequently caused confusion.
- 3.6 The previous approach to the quantification of Strategic Risk was to assess the financial impact of the risk against the Business Plan forecast; these specific amounts associated with each year of the Business plan forecast were aggregated to form a definitive quantitative value for each Strategic Risk. This is also being reviewed.

## **4 Risk Management Improvements**

### **Overview**

- 4.1 The key driver of this work is to ensure we adopt a continuous improvement approach to risk management and ensure this is embedded across the organisation as good business practice.
- 4.2 Work to date has focussed on four key areas:
  - (a) The procedure document should be the guide to all risk management across the business, but whilst the current document is concise and covers all of the main concepts, in certain areas it is incomplete, out of date or confusing;
  - (b) Strategic Risk is not well understood, certain concepts are muddled and key documents need refreshing and updating – see specific areas highlighted in the work undertaken on Strategic Risk Management that follows below;
  - (c) The link between Operational, Programme, Project and Strategic Risk needs to be better understood; and
  - (d) Our approach benchmarked against the industry standards – International Standard ISO 31000 (considering our process, procedures and methodology), the Treasury ‘Orange Book’ (checking our approach compared to public sector guidelines); and the UK Financial Reporting Council (‘FRC’) Risk Management Guide (2014) (looking at the themes and concepts used in larger commercial entities). In overall terms our approach covers the basics, but there are a number of key areas that need redefinition and refinement.

### **Strategic Risk Management: New Approach**

- 4.3 In response to the activity previously noted we have refreshed the TfL approach to Strategic Risk, in line with leading practice guidelines. The goal is to bring together and simplify Strategic Risk activities across the organisation. This enables management to focus on the agreed key Strategic Risks for TfL which should in turn help to provide benefits that include:
  - (a) greater likelihood of achieving strategic objectives;

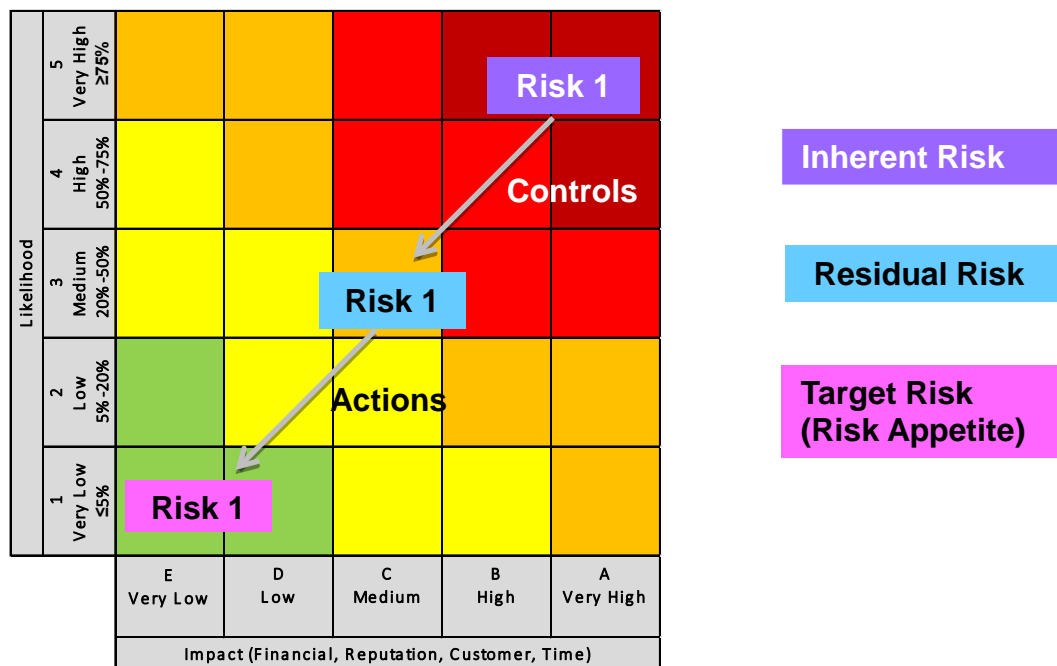
- (b) more systematic decision-making leading to better quality decisions;
  - (c) improved allocation of resources; and
  - (d) prioritised investment in the control infrastructure.
- 4.4 Going forward, the 'Risk Management in TfL' procedure document will provide a common framework for communication of risk management throughout the organisation. An updated risk terminology has been summarised in a revised Glossary of Risk Management Terms (see Appendix 1) to help ensure that risk related terms used in the methodology are properly understood and are used consistently.

### **Inherent, Residual and Target Risk**

- 4.5 The new approach continues to assess risk both quantitatively and qualitatively, but Strategic Risks will be assessed on an overall inherent basis - an approach that follows recognised best practice. Risk appetite is also being established for each of the Strategic Risks, to ensure that the planned actions are aligned with the risk appetite level.
- 4.6 Inherent risk is the assessment with no controls or other mitigating factors in place, which is the only way to assess the actual impact and reliance on controls and the strength of the control environment. By assessing our inherent risks and identifying controls, it is easier to check how much dependence there is on control activities, especially when determining the key or essential controls (those that may cover a critical risk or cover a number of risks).
- 4.7 The new reporting presentation aims to show the different relationship between inherent and residual risk. The risks will be reported visually in a new 'heat map' presentation so that the results of the risk assessments (i.e. likelihood and impact ratings) are represented in a graphical and concise way. The heat map shows the risk rating of different risks, and as noted above, the reliance on or strength of controls.
- 4.8 The relationship between inherent, residual and target risk is shown pictorially in Figure 1 overleaf. The concept applied follows a 5 step process:
- (a) The overall starting position is the risk if no controls or other mitigating factors are in place (i.e. our 'Inherent Risk'). This is why the 'Inherent' risk typically has a relatively high likelihood and impact positioning on the heat map.
  - (b) The existing 'controls' or management activities are identified and assessed in terms of design (*is it the best control?*) and operation (*does the control work?*) and this should reduce the likelihood and impact rating for the risk.
  - (c) This provides the 'residual' re-assessment of likelihood and impact – although it is not necessarily always a lower likelihood and impact positioning on the heat map as it depends on the effectiveness of the identified controls.

- (d) At this point a view is drawn as to the 'Risk Appetite' position – *are we happy to accept the net level of risk?* - if not 'Actions' may be determined which when implemented improve the control position (i.e. actions should become controls or a related management activity).
- (e) The final risk assessment is whether we have achieved our 'target' (which should be initially determined at level (i) above as the position we want to achieve), this again should more often show an even lower likelihood and impact - although given their nature some external risks may not move to a great extent as control activities can be difficult to undertake and may rely more on monitoring and influencing rather than controlling.

Figure 1: Relationship between inherent, residual and target risk



### Re-categorisation of Strategic Risks

- 4.9 The new categorisation aims to draw out the Strategic Risks which were previously masked in the broader Pan-TfL Risk categories. It will now be possible to focus on risk assessments and mitigating activities for each of the individual Strategic Risks which is important as these can be very different for each risk.

### Quantitative Assessment and Risk Rating

- 4.10 As outlined above, the previous approach to Strategic Risk Management attempted to establish an overall financial cost of any risk event or action based on the Business Plan forecast. This followed a mechanistic approach and resulted in an estimated exposure that was not tangible or useful for decision making.
- 4.11 Traditional risk management processes - outside of the sophisticated scenario planning undertaken in large financial institutions - struggle to determine a precise financial impact for all risks. Even a one-off catastrophic event will bring a range of hidden, unforeseen and reputational-based costs, as well as lost revenue opportunities.

- 4.12 The new approach considers the financial impact but under each assessment criteria ('Very Low' up to 'Very High') a range of financial or cost parameters are set (from less than £50 million [Very Low] up to over £1 billion [Very High]). Consequently, the approach has moved from time spent trying to achieve a precise figure to a position of estimating an overall worst case scenario, by applying practical assumptions and building in a degree of realistic flexibility.
- 4.13 The Strategic Risk rating approach has also been updated and the Risk Assessment Criteria to be used going forward includes the financial parameters noted above. The risk assessment table covers: Financial, Reputation, Customer and Time criteria from Very Low to Very High and the highest rating drives the overall impact rating. Risks are plotted on the heat map with a Scoring Scheme Criteria (see Appendices 2 and 3).

### **Application of the New Approach**

- 4.14 21 Strategic Risks have been previously identified. An initial desktop review of these risks indicates that some can be removed and/or amalgamated, which reduces the number to 14. This is set out in Appendix 4.
- 4.15 Individual risk data will be recorded in new Strategic Risk Forms which provide the information at each stage of the process outlined above. A blank example Strategic Risk Form template is provided in Appendix 5.

## **5 Next Steps**

- 5.1 After presenting an update to the Leadership Team, a follow-up interactive 'workshop' session is to be held at a Leadership Team Away Day, which will be facilitated by a risk specialist from E&Y. This will enable the Leadership Team to determine the key Strategic Risks in their area, as well as consider the broader pan TfL perspective.
- 5.2 A further workshop session will be scheduled with the Audit and Assurance Committee later this year to provide the Committee with the opportunity to review and discuss the Strategic Risks and determine whether any additional risks should be included.

### **List of appendices to this report:**

Appendix 1: Glossary of Risk Management Terms

Appendix 2: Risk Likelihood and Impact Criteria

Appendix 3: Risk Scoring Scheme Criteria

Appendix 4: Current Strategic Risks and revisions being discussed at Leadership Team Away Day

Appendix 5: Strategic Risk Form Template

**List of Background Papers:**

None

Contact Officer: Ian Nunn, Managing Director and Chief Finance Officer  
Number: 020 3054 8941  
Email: [IanNunn@tfl.gov.uk](mailto:IanNunn@tfl.gov.uk)

## Appendix 1 - Glossary of Risk Management Terms

---

### **Risk**

Risk is the threat that an event or action will adversely affect the organisation's ability to achieve its strategic objectives and maximise stakeholder value. Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

*[Note: The emphasis on the impact on objectives is important: a problem or hazard that cannot affect the organisation's objectives is not a risk relevant to that organisation. Therefore the starting point for any organisation considering its risks is to know very clearly what it is trying to achieve].*

### **Action**

Activity not yet in place but is planned or in progress in order to further reduce the likelihood and/or impact of the risk beyond the existing controls in place. The action should typically lead to a further control activity.

### **Asset Risk**

Asset risks are associated with the effective and efficient delivery of operational asset management objectives such as optimising the performance of assets and asset systems, and minimising whole life asset costs.

### **Assurance**

An evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.

### **Control**

Any process, policy, device, practice or other actions in place that is expected to reduce the likelihood or impact of the risk occurring.

### **Establishing the Context**

Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy

### **Exposure**

The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risk is realised.

---

## Appendix 1 - Glossary of Risk Management Terms

---

### **Inherent Risk**

Risk that an activity would pose if no controls or other mitigating factors were in place (this is the same as gross risk or risk before controls). Inherent Risk assumes adhering to specific regulatory or legal requirements.

### **Monitoring**

Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected – it can be applied to a risk management framework, risk management process, individual risk or control.

### **Operational Risk**

Operational risks are associated with the day to day provision of a transport service including support functions and impacts from external events.

### **Programme Risk**

Programme risks are associated with transforming strategic plans into actions relating to capital programmes comprising multiple, interdependent or interrelated projects.

### **Project Risk**

Project risks are associated with the risk management process supplemented in projects and programmes by a project risk management process. This is governed by the integrated projects and programme methodology ('TfL Pathway') and made available through the TfL Programme Management Office ('PMO').

### **Residual Risk**

Risk that remains after controls are taken into account (this is the same as net risk or risk after controls).

### **Risk Appetite**

The amount and type of risk that the organisation is willing to take in order to meet its strategic objectives (this may be compared in simple terms to Target risk).

### **Risk Category**

The Pan-TfL Risk Category that the risk most appropriately falls into –eg. TFL01 Maintaining a long term, strategic balanced plan.

---



## Appendix 1 - Glossary of Risk Management Terms

---

### **Risk Description**

A description of the risk, its cause and consequence if the risk were to occur.

### **Risk Heat Map**

A risk heat map is a tool used to present the results of a risk assessment process visually and in a meaningful and concise way. It involves evaluating the likelihood and potential impact of the identified risks.

### **Risk Identification**

The process of finding, recognising and describing risks, based on a review of strategic objectives, business processes, business unit activities, internal and external data, potential events and hazards and other relevant information.

### **Risk Impact**

The outcome of an event affecting business objectives, based on financial, time, reputation, customer and safety considerations.

### **Risk Likelihood**

The chance of something happening, expressed in both time cycle period and percentage terms.

### **Risk Management**

All of the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

### **Risk Management Framework**

A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

### **Risk Management Policy**

A statement of the overall intentions and direction of the organisation related to risk management.

---

## Appendix 1 - Glossary of Risk Management Terms

---

### **Risk Owner**

A person or entity with the accountability and authority to manage a risk.

### **Risk Theme**

The Pan-TfL Theme that the risk most appropriately falls into – e.g. Customer, People, Delivery, Value.

### **Risk Title**

Short title, or “headline” of the risk.

### **Risk Tolerance**

The amount and type of risk that an organisation is able to deal with.

### **Risk Treatment**

The process to modify a risk that results in an action and might include:

- *Treat* – take action to increase control activities
- *Transfer* – outsourcing the risk or buying cover via an insurance contract
- *Terminate* – exiting the activity as the risk is greater than business benefit
- *Tolerate* – the status quo of accepting the risk and current controls
- *Take* – de-control / take on more risk – could be assessed as an ‘opportunity’

### **Strategic Risk**

Strategic risks either affect or are created by an organisation’s business strategy and strategic objectives, and its relationship with its external and internal environment.

---

## Appendix 2 – Risk Likelihood and Impact Criteria

LIKELIHOOD – Once or more per year >75% (5)		
<b>IMPACT – Very High (A)</b>	<b>Financial</b>	<b>(A) &gt;£1 billion</b>
	<b>Time</b>	<b>&gt;52 weeks delay</b>
	<b>Reputation</b>	<p>Risk results in significant ongoing negative media coverage &amp; major loss of confidence/ significant intrusion by regulators/ stakeholders leading to one of the following outcomes:</p> <ul style="list-style-type: none"> <li>• Fundamental changes to the TfL operating model/structures</li> <li>• High profile management changes (e.g. Managing Directors MDs)</li> <li>• Fundamental changes to safety procedures</li> </ul>
	<b>Customer</b>	<p>Impact on multiple modes of transport as a result of more than one of the following:</p> <ul style="list-style-type: none"> <li>• Full/part line suspension of more than 1 line for more than 1 day</li> <li>• Negative impact on journey time reliability at peak periods affecting a high number of high flow corridors on the TfL Road Network (TLRN) and occurs more than once a week over the course of several weeks</li> <li>• Full/part line suspension on 1 line for more than a week</li> <li>• Severe over crowding of affected areas of the bus network, contributing to higher safety risks</li> <li>• Very high impact on non time elements of customers journeys e.g. ambience, staff customer service, information sufficient to cause loss of more than two points to the CSS score in the operating business</li> </ul>
LIKELIHOOD - Once or more in 2 years >50-75% (4)		
<b>IMPACT – High (B)</b>	<b>Financial</b>	<b>(B) £500 million - £1 billion</b>
	<b>Time</b>	<b>26-52 weeks delay</b>
	<b>Reputation</b>	<p>Risk results in ongoing negative media coverage &amp; loss of confidence/significant intrusion by regulators/stakeholders leading to one of the following outcomes:</p> <ul style="list-style-type: none"> <li>• Sustained (i.e. one week+) diversion of MDs and senior managers' time, energy &amp; resources away from business as usual activities &amp; planned projects, to deal with feedback</li> <li>• Loss of support leading to removal of key funding</li> <li>• Loss of trust leading to fundamental changes to governance arrangement.</li> <li>• Series of strikes impacting operations (bus or tube network)</li> </ul>
	<b>Customer</b>	<p>Impact on multiple modes of transport:</p> <ul style="list-style-type: none"> <li>• Negative impact on journey time reliability at peak periods affecting a number of high flow corridors on the TLRN and occurs more than once a week for a few weeks</li> <li>• Full, or part line suspension for more than 1 line for a whole day</li> <li>• Full or part line suspension on 1 line for several days</li> <li>• Severe over crowding of affected areas of the bus network, contributing to higher safety risks</li> <li>• High impact on non-time elements of customers journeys e.g. ambience, staff customer service, information sufficient to cause loss of CSS KPI score in the operating businesses.</li> </ul>
LIKELIHOOD - Between once in 2 to once in 5 years >20-50% (3)		

## Appendix 2 – Risk Likelihood and Impact Criteria

<b>IMPACT – Medium (C)</b>	<b>Financial</b>	<b>(C) £100 million - £500 million</b>
	<b>Time</b>	<b>12-26 weeks delay</b>
	<b>Reputation</b>	<p>Risk results in negative media coverage &amp; loss of confidence/increase intrusion by regulators/stakeholders leading to one of the following outcomes:</p> <ul style="list-style-type: none"> <li>• Short-term (less than one week) diversion of MDs and senior managers' time, energy and resources away from BAU activities, &amp; planned projects to deal with feedback</li> <li>• Sustained (i.e. more than one week) diversion of middle managers' time, energy and resources away from BAU activities and planned projects, to deal with feedback.</li> <li>• Limited industrial actions such as a one-off strike or local strikes impacting operations (i.e. trains cancelled and/or stations closed)</li> </ul>
	<b>Customer</b>	<p>More than one of the following impacting on multiple modes of transport:</p> <ul style="list-style-type: none"> <li>• Full/part suspension or failed Depot access</li> <li>• Repeated severe delays (= severe delays occurring more than once over the course of the week)</li> <li>• Negative impact on journey time reliability occurring more than once a week at peak periods on the TLRN</li> <li>• Over crowding of some affected areas of the bus network, contributing to higher safety risks</li> <li>• Journey time exceeds the target for "Excess Wait Time" once a week for several weeks on a number of High Frequency routes</li> <li>• Impact of non-time elements of customers journeys e.g. ambience, staff customer service, information - sufficient to cause loss of CSS KPI</li> </ul>

<b>LIKELIHOOD - Less than once in 5 years &gt;5-20% (2)</b>		
<b>IMPACT - LOW (D)</b>	<b>Financial</b>	<b>(D) £50 million - £100 million</b>
	<b>Time</b>	<b>4-12 weeks delay</b>
	<b>Reputation</b>	<p>Risk results in short term negative media coverage or impact on relations with regulators/stakeholders leading to one of the following outcomes:</p> <ul style="list-style-type: none"> <li>• Significant negative feedback from customers via the Customer Service Centre or from stakeholders via media outlets (Twitter, blog etc.)</li> <li>• Short-term (less than one week) diversion of middle managers' time, energy &amp; resources away from BAU activities &amp; planned projects</li> <li>• Unions building a case for action</li> </ul>
	<b>Customer</b>	<p>Low impact to services across multiple modes:</p> <ul style="list-style-type: none"> <li>• Major delay (once instance of severe delay) on a line or repeated minor delays occurring daily over the course of a week</li> <li>• No impact to overall journey time reliability, however localised impact to a number of high flow corridors on the TLRN</li> <li>• Major station closure or over crowding on localised routes affected by disruption</li> <li>• Journey time exceeds the target for "Excess Wait Time" once a week for several weeks on a small number of High Frequency routes</li> <li>• Impact on non-time elements of customers journeys e.g. ambience, customer staff service, information - decreases in individual elements of CSS without loss of the KPI</li> </ul>

## Appendix 2 – Risk Likelihood and Impact Criteria

LIKELIHOOD - Less than once in 20 years <=5% (1)		
IMPACT - VERY LOW (E)	Financial	(E) <£50 million
	Time	<4 weeks delay
	Reputation	Risk has negligible impact on regulators/ stakeholders but does impact customers & employees leading to one of the following outcomes: <ul style="list-style-type: none"> <li>Low level of negative feedback from customers via the Customer Service Centre or from stakeholders via media outlets -(Twitter, blogs)</li> </ul>
	Customer	Negligible impact across any mode of transport: <ul style="list-style-type: none"> <li>No impact to overall journey time reliability however localised impact to a small number of high flow corridors on the TLRN</li> <li>Minor delay or closure of a major station</li> <li>Negligible impact on non-time elements of customers journeys e.g. ambience, staff customer service, information, negligible impact on individual elements of CSS KPI and no impact on KPI score</li> </ul>

### Appendix 3 – Risk Scoring Scheme Criteria

Likelihood	5 Very High ≥75%	11	16	20	23	25
	4 High 50%-75%	7	12	18	21	24
	3 Medium 20%-50%	4	8	13	19	22
	2 Low 5%-20%	2	5	9	14	17
	1 Very Low ≤5%	1	3	6	10	15
		E Very Low	D Low	C Medium	B High	A Very High
Impact (Financial, Reputation, Customer, Time)						

# Current Strategic Risks and revisions being discussed at Leadership Team Away Day

## Current 21 Strategic Risks

1	Change to Central Government Funding
2	Change to Business Rates
3	Variability of Fares Income
4	Volatility in Capital Market
5	Secondary Revenue Target not achieved
6	Non delivery of cost savings and efficiencies
7	Planning projects without allocated funding
8	Shortfall in Crossrail funding contributions
9	Loss of key people
10	Strike Action
11	Future TfL pension fund deficit
12	Non delivery of key elements of investment programmes
13	Loss of key IT system
14	Cyber attack
15	Increased road congestion and deteriorating bus reliability
16	Operational targets not achieved
17	Loss from reliance on major supplier
18	Non achievement of Mayor's road safety targets
19	Non achievement of Mayor's target for growth in cycling
20	TfL's portion of EU air quality targets not achieved
21	Catastrophic event



## Proposed 14 Strategic Risks

Proposed 14 Strategic Risks		Maps to
1	Major unplanned loss of revenues	1,2,3
2	Volatility in Capital Market	4
3	Secondary Revenue Target not achieved	5
4	Shortfall in Crossrail funding contributions	8
5	Loss of key people	9
6	Strike action	10
7	Future TfL pension fund deficit	11
8	Non delivery of key elements of investment programmes	12
9	Loss of key IT system	13
10	Cyber attack	14
11	Operational targets not achieved	16
12	Loss from reliance on major supplier	17
13	TfL's portion of EU air quality targets not achieved	20
14	Catastrophic event	21

### Removed previous risks:

6, 7, 15, 18 and 19

- Risks 7, 15, 18 and 19 were removed as it was considered that these are not strategic risks facing TfL and are more operational in nature.
- Risk 6 has been removed due to significant changes made to the Savings and Efficiencies Programme and so a separate risk is not required.

## Appendix 5 – Strategic Risk Form Template

<b>Strategic Risk:</b>	
<b>Risk Description:</b>	
<b>Risk Reference:</b>	<b>Risk Owner:</b>
<b>Risk Category:</b>	

Inherent Risk	Risk Assessment	Inherent Rationale
<i>Likelihood</i>		
<i>Overall Impact</i>		
<i>Risk Rating – Lowest (1) to Highest (25)</i>		

Number of Controls	Overall Effectiveness Rating (Effective, Partially Effective, Ineffective)
--------------------	-------------------------------------------------------------------------------

Residual Risk	Risk Assessment	Residual Rationale
<i>Likelihood</i>		<i>Financial Impact</i>
		<i>Reputation Impact</i>
		<i>Customer Impact</i>
		<i>Time Impact</i>
<i>Overall impact</i>		
<i>Risk Rating – Lowest (1) to Highest (25)</i>		

Risk Treatment Conclusion	
---------------------------	--

Number of Actions	Number of Overdue Actions
-------------------	---------------------------

Risk Target	Risk Assessment	Target Rationale
<i>Likelihood</i>		
<i>Overall Impact</i>		
<i>Risk Rating – Lowest (1) to Highest (25)</i>		

Assessed: Month / Year



## Appendix 5 – Strategic Risk Form Template

<b>Control Description</b> (Key controls highlighted in blue)	<i>Control Owner</i>	<i>Frequency</i>	<i>Design</i>	<i>Operation</i>	<i>Rating</i>

<b>Action Description</b>	<b>Action Owner</b>	<b>Action Date</b>

Assessed: Month /Year