Audit and Assurance Committee

Date: **14 March 2024**

Item: **Enterprise Risk Update – Governance and Controls Suitability (ER10)**

This paper will be considered in public

1 Summary

1.1 As part of Transport for London's (TfL) risk management process, Enterprise Risk 10 – Governance and Controls Suitability (ER10) is allocated to this Committee for its review and oversight.

1.2 ER10 assesses whether TfL's governance and controls are fit for purpose and if they provide adequate support to meet the changing demands on TfL and expectations of our stakeholders.

1.3 This paper provides an overview of ER10 and how it is managed. The top three key mitigations to move from Current to Target position for ER10 are: Privacy and Security; TfL's Management System; and Governance Framework including TfL's Board, Committees and Panels. Further detail of these mitigations is set out in section 4.1 below.

1.4 An appendix is included on Part 2 of the agenda which contains supplementary information that is exempt from publication by virtue of paragraph 3 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to the business affairs of TfL. Any discussion of that exempt information must take place after the press and public have been excluded from this meeting.

2 Recommendation

2.1 **The Committee is asked to note the paper and the exempt supplementary information on Part 2 of the agenda.**

3 Current Status

3.1 The current probability of the risk occurring remains Low due to the design and effectiveness of the controls and arrangements in place, including dedicated teams that oversee TfL's governance arrangements, controls and their suitability. The probability is also Low based on the greater scrutiny and regulation of data controls and data loss and compliance with procurement processes. Our target is to reduce the probability to Very Low.

3.2 The overall risk score remains Medium but with key mitigations our target is to reduce risk exposure to Low.

3.3 The overall control effectiveness rating for ER10 is Adequately Controlled as controls are designed correctly and are in place and further actions have been identified to improve the effectiveness of certain controls. The probability and impact of the risk and the control measures to address it are regularly reviewed and are always reassessed following any significant issues arising relating to governance or any actions arising from a related audit report.

3.4 The key causes that relate to risk exposure are: not being aware of or following appropriate processes, or processes being inadequate or not available; failure to seek appropriate approvals for decisions; not keeping up to date with changes that affect our governance arrangements (e.g. changes in legislation and compliance with legal requirements); failure to comply with and update strategic controls; and ineffective controls or failure of control measures.

3.5 The potential consequences of this risk materialisation have been identified as: reputational damage; transactions and projects operating without appropriate approval or oversight; possible financial loss from third parties; regulatory action and/or penalties due to breach of regulations; and safety, health or environmental damage due to incidents/ accidents occurring as a result of inappropriate or ineffective governance and decision making.

3.6 Financial impact remains Very High based on potentially high fines or costs owed if TfL were to be fined, for example due to a data breach.

4 Controls and Mitigation

4.1 A large number of actions and controls are in place to mitigate the risk. Overall, the top three mitigations for ER10 are:

(a) **Privacy and Security:** We have a business-as-usual privacy and data protection compliance programme of activities to maintain and support compliance across TfL with the UK General Data Protection Regulation (GDPR) requirements. There have also been no instances of non-compliance with GDPR that have resulted in enforcement action by the Information Commissioner's Office. We are also working with other areas of the business on the programme of security and information governance mandatory training courses for all staff. As such, this ongoing preventative control has been assessed as effective for both design and operation.

Since the last update to the Committee, we have added this control and removed the previous Privacy and Data Protection Compliance Programme ongoing preventative control.

(b) **TfL's Management System (TMS):** The TMS is where all colleagues can find TfL's policies and procedures online and, as part of the Our TfL Programme (OTP), a programme of tactical improvements to strengthen the TMS has been developed and is currently in delivery. We are also continuing with our programme of regular review and update of existing content.

This ongoing preventative control has been assessed as effective for design and partially effective for operation but following completion of improvements identified through OTP we expect to improve this rating to effective.

(c) **Governance Framework including TfL's Board, Committees and Panels:** A governance framework is in place and audits are undertaken by the Risk and Assurance Directorate to ensure that all areas of TfL are complying with it. Any governance issues identified from audits are reported to the Committee as part of the Quarterly Risk and Assurance Update and, where applicable, as part of the Annual Governance Statement. Delegated decision making and organisational governance is regularly reviewed in light of experience, organisational requirements, changed circumstances and changes in legal requirements or professional standards and guidance.

The Terms of Reference and oversight of TfL Board, Committees and Panels are kept under regular review and changes made when necessary (this included standing down the special purpose Elizabeth Line Committee in July 2023 following close out of the Crossrail project). The recommendations from the externally led Board Effectiveness Review for 2023 were reported to the October 2023 Board meeting and actions are being implemented. An update will be provided as part of the Annual Governance Statement and the governance improvement plan approval paper to the June 2024 meeting of the Committee. Preparations are also taking place for a Board recruitment campaign which will commence in April 2024.

This ongoing preventative control has been assessed as effective for both design and operation. This control now combines the previously separate Governance Framework, and Board, Committees and Panels controls, which were also both effective for design and operation.

4.2 In addition to the three preventive controls set out above, there are 22 further controls – 13 of which are preventative and nine corrective. The nine corrective controls remain effective for both design and operation.

4.3 Since the last update to the Committee, we have added the following six ongoing preventative controls:

(a) Cyber Security Strategy – this replaces the previous Cybersecurity Programme control and has been assessed as effective for design and partially effective for operation as there is an action to review and update the Strategy;

(b) Gifts and Hospitality Process and Procedure – this has been assessed as partially effective for both design and operation while we address actions from an internal audit;

(c) Sufficient Legal Resource – this has been assessed as effective for both design and operation;

(d) Declarations of Interest Process and Procedure – this has been assessed as effective for both design and operation but we are also looking to source a suitable automated system to record and track declaration responses which will strengthen the process further;

(e) Risk Management Policy, Procedure and the Enterprise Risk Management Framework – this has been assessed as effective for design and partially

effective for operation but following an update of the policy and procedure by the end of June 2024 we expect to improve this rating to effective; and

(f) Risk Management Awareness Training – this has been assessed as effective for design and partially effective for operation but following an update of the internal e-learning course by the end of June 2024 we expect to improve this rating to effective.

4.4 The following two ongoing preventative controls are now assessed as effective for both design and operation:

(a) the Annual Governance Statement, for inclusion in the Annual Report, is recorded as effective as most actions are ongoing and all are being addressed and the statement is signed off by our external auditors each year; and

(b) TfL's Standing Orders are regularly reviewed and changes made when necessary to ensure the effectiveness of decision making so that decisions are as robust as possible to legal challenge. These were updated in October 2023.

4.5 Of the remaining five preventative controls, all continue to be assessed as effective for both design and operation:

(a) communication of election guidance across TfL;

(b) transparency and strategic policy and publications framework;

(c) annual Board Effectiveness Reviews with an independent review every three years;

(d) Greater London Authority and London Assembly oversight; and

(e) delivery of the Integrated Assurance Plan, monitoring of the completion of actions and reporting to the Board's Committees and Panels.

4.6 Level 1 governance risks have been identified and development of these risks are progressing, which will ensure that there is a clear line of sight of governance risk at all levels of the organisation.

List of appendices to this report:

A paper containing exempt supplemental information is included on Part 2 of the agenda.

List of Background Papers:

None

Contact Officer: Andrea Clarke, Interim General Counsel
Email: andreaclarke@tfl.gov.uk