Audit and Assurance Committee

Date: **16 March 2022**

Title: **Enterprise Risk Update - Governance Controls and Suitability (ER13)**

This paper will be considered in public

1 Summary

1.1 This paper provides an overview of the Level 0 Enterprise Risk 13 – "Governance and controls suitability" (ER13).

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

3 Risk Assessment

3.1 ER13 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.

3.2 The key causes that relate to risk exposure for ER13 are: not being aware of or following appropriate processes; failure to seek appropriate approvals for decisions; not keeping up to date with changes that affect our governance arrangements (eg changes in legislation); failure to comply with and update strategic controls; and ineffective controls or failure of control measures.

3.3 The key consequences could be: 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 (SHE) damage due to incidents/accidents occurring as a result of inappropriate or ineffective governance and decision-making.

3.4 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. Following a recent review, the current probability of the risk occurring increased from very low to low, based on the greater scrutiny and regulation of data controls and data loss and compliance with procurement processes. Due to adequate

controls being in place, the current and target SHE impacts were reduced from medium to very low, Customer/Stakeholder impacts were reduced from medium to low and Stakeholder Confidence impacts were reduced from high to low.

3.5 Current Finance impact increased from medium to very high and the target Finance impact increased from medium to high, both changes made based on TfL's current funding position. This has led to an increase in the overall current risk score and Finance impact being out of tolerance level.

3.6 Overall control effectiveness rating continues to be 'Adequately controlled' as all controls are designed correctly, are in place and are operating effectively.

4 Controls and Mitigation

4.1 Twenty-two controls have been identified – 13 preventative and nine corrective. All nine corrective controls have been assessed as effective for both design and operation.

4.2 Of the 13 preventative controls, seven were assessed as effective for both design and operations and these are:

(a) Governance Framework;

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

(c) Terms of Reference and oversight of the TfL Board, Committees and Panels are kept under regular review and changes made when necessary;

(d) Greater London Authority and London Assembly oversight;

(e) transparency and strategic policy and publications framework;

(f) annual Board effectiveness reviews with an independent review every three years; and

(g) communication of election guidance.

4.3 The remaining six preventative controls assessed as effective for design but partially effective for operation are:

(a) Standing Orders;

(b) TfL's Management System (TfL policies, controls and processes);

(c) privacy and data protection compliance programme;

(d) cybersecurity programme;

(e) Governance Statement for the Annual Report (includes the Governance Improvement Plan); and

(f) TfL's Enterprise Risk Management Framework.

4.4 The below table provides a summary of various actions taken to further reduce risk exposure.

Key Issue	Action
Effectiveness of decision-making	**Ongoing:** TfL's Standing Orders are kept under regular review and changes made when necessary to ensure the effectiveness of decision-making so that decisions are as robust as possible to legal challenge. A Board review of the effectiveness of its decision-making is conducted each year and the outcome of the 2021 review was discussed at the 8 December 2021 Board meeting. Delegated decision-making and organisational governance is regularly reviewed in the light of experience, organisational requirements, changed circumstances and changes in legal requirements or professional standards and guidance. An externally led review will be commissioned for 2022.
TfL's Management System	**Ongoing:** We continue to engage with various business areas to ensure that relevant content currently outside the system, for example policies that apply to all staff, is included in the Management System. Trams, Surface (Assets), Technology & Data, Finance and SHE are currently creating and/or migrating new content. Attention is also focussed on reviewing and updating existing content.
Privacy and data protection	**Ongoing:** Verification, input and refresh of mapping of personal data continues and plans have been implemented for regular data refresh. **Ongoing:** Regular assurance is sought from key suppliers that they are complying with their data protection obligations. **Completed:** Our Data Protection Impact Assessment template has been updated. **Completed:** The Information Commissioner's Office Age Appropriate Design Code came into force on 2 September 2020 with a 12-month transition period. We identified and logged issues relating to the code and internal guidance was developed and is available in the Management System. **In progress:** A table top exercise to test personal data breach and incident management processes forms part of the planned resilience activity that will be delivered under the Cyber Security Strategy. In September 2021, Cyber Security held the first of a series of incident management exercises which included testing that incident management process on a basic level is done. A personal data breach will be a focus of a later exercise in 2022.

Key Issue	Action
Coordinated approach to Digital Accessibility across TfL	**In progress:** A co-ordinated set of measures were implemented to achieve compliance with the Digital Accessibility Regulations, which took full effect on 23 September 2020, and these continue to be worked through.
Annual Governance Statement (including the Governance Improvement Plan)	**Completed:** A review of compliance with the TfL Code of Governance in 2020/21 was presented to the Committee at the 7 June 2021 meeting. The Committee also: approved the Annual Governance Statement, for inclusion in TfL's 2020/21 Annual Report and Accounts; noted the progress against the 2020/21 Governance Improvement Plan; and approved the 2021/22 Governance Improvement Plan.
TfL's Enterprise Risk Management Framework	**Ongoing:** TfL's Enterprise Risk management processes are well established and are regularly reviewed to ensure they are fully effective. We are on track to meet our commitment to the TfL Board to have the 14 Enterprise Risks reviewed by the relevant Committee or Panel by 2021/22 year end.

4.5 Some of the above key issues are included in the 2021/22 Governance Improvement Plan, approved by the Committee at its meeting on 7 June 2021. We are also in the processes of reviewing a number of aspects of our governance arrangements as part of the implementation of the recent changes to the Executive Committee and to ensure the ongoing efficiency and effectiveness of our internal control procedures.

5 Internal Audit Reviews

5.1 To date Internal Audit has completed one review, with three in progress, of matters that fall within the scope of ER13. The three reviews in progress refer to Declarations of Interest, Recruitment and TfL Procurement and Supply Chain Capacity to take on the procurement of the Elizabeth line's existing contracts and recruitment.

5.2 The completed review was in response to the Department for Business, Energy & Industrial Strategy consultation 'Restoring trust in audit and corporate governance' (the White Paper). This set out a package of measures aimed at improving the UK's audit, corporate reporting, and corporate governance systems. The objective of the audit was to assess the proposals made in the White Paper, identify whether it contained any proposals that would either impact directly on TfL, or had the potential to be adopted as good practice by TfL. This follows previous internal audit work on the associated Brydon report.

5.3 The proposals within the White Paper were still in the consultation period with no guarantee as to which would become regulatory or legal requirements. The Internal Audit review highlighted a number of cases where TfL currently does not meet the requirements of proposed regulatory or legal changes, and where work may be required to achieve future compliance. As the White Paper is primarily focused on the external audit process with only brief mention of internal audit, we did not consider there to be any significant implications for the work of the TfL Internal Audit team.

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: Howard Carter, General Counsel
Email: howardcarter@tfl.gov.uk