Audit and Assurance Committee

Date: **15 September 2021**

Item: **Risk and Assurance Quarter 1 Report 2021/22**

This paper will be considered in public

1 Summary

1.1 The purpose of this report is to inform the Committee of the work completed by the Risk and Assurance Directorate during Quarter 1 of 2021/22 (Q1), the work in progress and planned to start, and other information about the Directorate's activities.

1.2 A paper is included on Part 2 of the agenda, which contains exempt supplemental information that is exempt from publication by virtue of paragraphs 3, 5 and 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to the business and financial affairs of TfL, that is commercially sensitive and likely to prejudice TfL's commercial position; and information relating to ongoing fraud and criminal investigations and the disclosure of this information is likely to prejudice the prevention or detection of crime and the apprehension or prosecution of offenders. 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 report and the supplemental information on Part 2 of the agenda.**

3 Director Update

3.1 This is the first quarterly report for 2021/22 to the Committee highlighting the activities of the five teams making up the Risk and Assurance Directorate, namely: Enterprise Risk; Internal Audit; Integrated Assurance; Project Assurance; and Counter-fraud and Corruption.

3.2 In this quarter the audit work is behind programme as a result of resource issues mainly relating to the number of staff vacancies in the teams (full details are provided in section 8 below) and audit work carried over from the previous financial year. Recovery plans and reprioritisation of work is underway to assess the full impacts on the audit programme so a risk-based approach can be taken in relation to allocation of resources.

3.3 Work has also begun on a number of initiatives to improve the effectiveness of the Directorate. These include staff engagement sessions to seek feedback on how the Directorate is working which were very beneficial and are being acted on by each head of team. Other initiatives include forming a collaboration working group to further improve how the teams in Risk and Assurance can work even

more effectively together. We are also looking at reporting, audit planning and interaction with key stakeholders.

3.4 Another key workstream underway is ensuring that themes and issues identified in the work of all the teams can be pulled together to better inform how we plan our work and inform the controls and mitigations on Enterprise and Level 1 Risks.

3.5 Good progress has also been made with the Safety, Health and Environment Directorate on strengthening the integration of second line assurance work between our two Directorates and a joint paper was recently submitted to the Safety, Sustainability and Human Resources Panel to explain how that work will be taken forward. Further progress updates will be provided to the Panel.

3.6 Following the identified trend in increases in Poorly Controlled (PC) and Requires Improvement (RI) outcomes over the past three years, the teams undertook an exercise to identify underlying reasons for this. Findings are as follows:

(a) Internal Audit

There is a clear year on year increase in the number of audit reports issued with either a RI or PC rating. Excluding memos, this rises in each year as follows: 2018/19 41 per cent, 2019/20 63 per cent and 2020/21 83 per cent. Reviewing the rates in different business areas indicated that in those three years, Crossrail had a higher proportion of reports being issued with a RI rating in comparison to the previous year (2018/19 zero per cent, 2019/20 14 per cent and 2020/21 21 per cent). Other areas either fluctuate or are steady and fluctuations were either due to our risk-based approach or the inconsistent number of reviews completed in each area.

Assessment was then carried out against the Enterprise Risk (ER) these reports were issued in over the three years. This again showed ER14 (Opening of the Elizabeth Line) as progressively getting more RI over the three years.

(b) Integrated Assurance

The analysis indicated that there is no real trend evident in RI and PC reports issued in the past three years, either by area or Enterprise Risk level. Percentages are fairly consistent and do not fluctuate greatly.

3.7 This analysis will be carried out on a regular basis, with findings reported as part of the Risk and Assurance quarterly reports and Annual Report.

3.8 Work has also begun on ensuring that trends across all teams in Risk and Assurance can be identified. Work is currently at different levels of maturity in each team but the aim is get each team to the same level and ensure this can then feed into work planning across the Directorate.

3.9 The planned integration of the Crossrail Project Programme Assurance team into TfL Risk and Assurance to cover all Elizabeth line functions rather than just Crossrail is covered elsewhere on the agenda.

4 Enterprise Risk Management

4.1 The following Level 0 Enterprise Risks reviews were facilitated by the team in the last quarter and the outcomes will now go forward to the relevant Panels and Committees as per the agreed schedule:

(a) Protecting the wellbeing of our employees (ER2);

(b) Cyber and protective security (ER4);

(c) Inability to support new ways of working (ER10); and

(d) Disparity leading to unequal or unfair outcomes (ER11).

4.2 It has been agreed that the focus of ER2 (Protecting the wellbeing of our employees) will extend to include the attraction and retention of staff to reflect the current challenges we face as an organisation.

4.3 The top five Strategic Level 1 risks for Elizabeth line have been agreed in principle. Workshops are underway to develop these further in terms of full risk assessments and mitigation strategies. Development of these risks is planned to be complete by December 2021 at the latest.

4.4 Integration of the Enterprise Risk Management and IT Information Security Risk Management processes are under way in line with ISO 27005 compliance.

4.5 Work undertaken on risk interconnectivity has been beneficial to the risk management process in several ways:

(a) The interconnectivity between Level 0 (Enterprise) and Level 1 (Strategic) risks have enabled us to complete a gap analysis on security and asset management risks across the organisation and has helped to shape our risk approach in these areas.

(b) The materialisation of highly interconnected risks may impact on several areas across the business. This type of modelling can aid risk scenario planning to strengthen systemic/strategic controls.

(c) The visual representation of risks including the overall control rating, impact, likelihood and levels of interconnectivity across the organisation is an effective risk communication tool for risk workshops, risk prioritisation, risk reporting and assurance planning.

4.6 A list of the Level 0 and Level 1 risks is included in Appendix 1.

5 Audit and Assurance

5.1 In TfL, assurance is delivered in accordance with the ‘three lines of defence’ model:

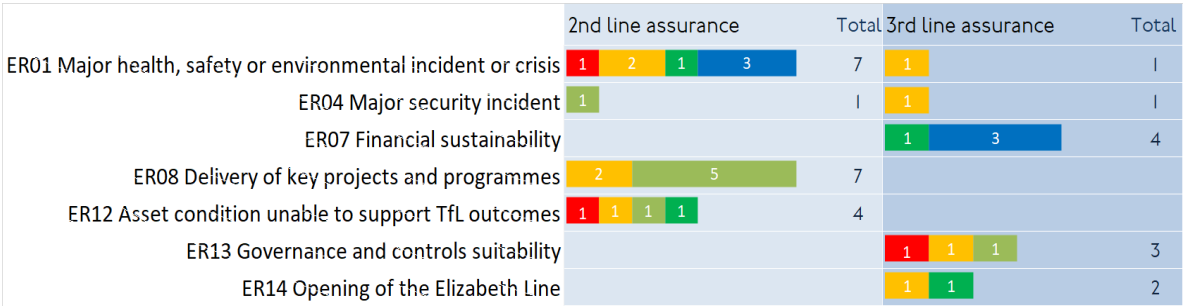
(a) First line of defence – control and monitoring arrangements carried out by the functions responsible for managing the risks/controls;

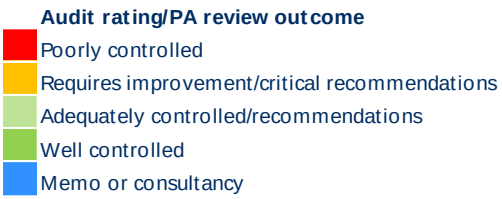
(b) Second line of defence – typically audit and inspection regimes carried out by teams separate from those responsible for managing the risks/controls, but reporting through the TfL management hierarchy; and

(c) Third line of defence – fully independent audit and review activities, typically with a strategic focus, and reporting to Executive Committee, Audit and Assurance Committee and other Board Committees and Panels.

5.2 Within the Risk and Assurance Directorate, the Internal Audit function provides third line assurance, whilst the Integrated Assurance and Project Assurance teams provide second line assurance. Further information regarding the work of these teams during Q1 is set out below.

5.3 The table below maps the outcomes of audit and project assurance reviews carried out by the teams in Risk and Assurance up to the end of Q1 against the TfL Enterprise Risks. (If a risk is not listed, this means that no work has been completed against it during the year so far).





Internal Audit

5.4 The Internal Audit plan forms part of the integrated assurance plan that the Committee approved on 17 March 2021.

5.5 A full list of audit reports issued during Q1 is included as Appendix 2. Audits in progress at the end of Q1 is included as Appendix 3, work planned to start in Q2 is included as Appendix 4, and details of changes to the audit plan is included as Appendix 5.

5.6 The Internal Audit Q1 summary, included as Appendix 6, includes highlights from work completed during the quarter. It also provides an overview of the delivery of the audit plan, a summary of the reports issued and conclusions and information on overdue audit actions.

5.7 At the last Committee we reported on the review being undertaken of the Department for Business, Energy and Industrial Strategy (BEIS) White Paper and its possible impact on TfL. This has now been completed and there are a number

of areas that would impact TfL should this become legislation. A TfL wide response was prepared and submitted to BEIS.

Mayoral Directions

5.8 Mayoral Directions fall into three broad categories: those addressing technical issues relating to statutory powers; those related to commercial development activities; and those related to projects and programmes.

5.9 On 30 November 2020, the Mayor directed TfL to provide direct financial assistance of up to £500,000 to the traders from Seven Sisters Market (MD2724). The financial support was intended to see the traders through the transition period since the closure of the TfL owned building that housed the market and the provision of a temporary market at Apex Gardens in 2021 (reported to the Board on 9 December 2020, the Finance Committee on 10 March 2021 and this Committee on 17 March 2021).

5.10 On 5 August 2021, Grainger withdrew from the Seven Sisters regeneration project, including the installation of a temporary market at Apex Gardens. Although TfL is progressing plans for a separate temporary market, traders face a further period where they are unable to trade. On 31 August 2021, the Mayor directed TfL to provide further financial support across all traders up to £500,000 (MD2868). This Mayoral Direction will also be reported to the Finance Committee on 6 October 2021 and to the Board on 20 October 2021.

Management Actions

5.11 The team monitors the completion of all Internal Audit management actions and confirms whether management has adequately addressed them. We report by Directorate on the percentage of actions closed on time over the past six periods. Appendix 6 provides additional information relating to action management trends over the last six periods.

5.12 This Appendix also includes information on overdue actions at the end of Q1. There were no actions arising from Internal Audits more than 60 days overdue at that date.

Integrated Assurance

5.13 The Integrated Assurance team carries out second line of defence audits, primarily in relation to health and safety and engineering compliance, and compliance with Payment Card Industry Data Security Standard (PCI DSS). Audit reports issued by the team follow a similar system of audit conclusions and priority ratings for issues as the Internal Audit team.

5.14 A summary of work carried out by Integrated Assurance in Q1 is included as Appendix 7.

5.15 In Q1, three audits were identified (two PC and one RI) that contained examples of non-compliance with the project management system and CDM (Construction Design and Management Regulations) requirements that had not been identified and corrected by first line controls. Consequently, Risk and Assurance met with the relevant members of Programme Management Office and a review has begun

of how the applicable controls are assured and the alignment and interaction of the different Directorates involved. The work involves mapping the applicable management systems and ensuring that the roles and responsibilities are clear in terms of who owns the systems and how they are assured from a holistic, rather than system specific perspective. Where gaps or overlaps are identified these will be addressed with the relevant teams.

5.16 All overdue actions have been raised with the action owners and the relevant line managers. To address the trend noted in the past year, Integrated Assurance (along with other Risk and Assurance teams) have improved the reporting to TfL leadership teams. This will ensure the senior teams are aware of audit findings and overdue audit actions at periodic and quarterly intervals which should help reduce the number of overdue actions.

Project Assurance

5.17 The Project Assurance team carries out assurance reviews of projects and programmes across TfL's Investment Programme, with individual projects selected for review following a risk-based assessment. Generally, projects with an Estimated Final Cost over £50m are also subject to (third line) input from the Independent Investment Programme Advisory Group (IIPAG). However, IIPAG's agreed work-bank is determined by the project's risk profile, which includes some projects less than £50m, and not all sub-programmes are reviewed. The IIPAG Quarterly Report is included elsewhere on the agenda. Reports from Project Assurance reviews are considered alongside the Authority request at the sub-programme board or operating business board depending on the size of the project.

5.18 Project Assurance also conducts reviews of the sub-programmes to inform annual requests for Authority at the Programmes and Investment Committee.

5.19 Project Assurance reviews do not carry an overall conclusion in the same way as audit reports, however, issues raised may be designated as critical issues. The Project Assurance team follows up on all recommendations to ensure they have been addressed and reports on those that are overdue to the Programmes and Investment Committee.

5.20 A summary of the work completed by Project Assurance in Q1 is included as Appendix 8. This Appendix also includes information on the themes that have been identified during the quarter and these are being discussed with senior officers to resolve.

Customer Feedback

5.21 There were 11 customer feedback forms (CFFs) returned in Q1. Internal Audit issued 11 questionnaires of which four were returned (36 per cent). Integrated Assurance issued 16 questionnaires of which seven were returned (44 per cent). A summary of customer feedback forms is included as Appendix 9.

5.22 We have noticed that the response rate to CFFs has gone down since Q1 2018/19 (72 per cent) and Q1 2019/20 (63 per cent). Reminders are sent to recipients of CFFs two weeks after receiving no response. We are therefore looking at further changes to how CFFs are sent and followed up, with the aim of

increasing the response rate. Whilst the response rate has reduced it is good to report that the scores received remain high at around 90 per cent.

6 Counter-Fraud and Corruption

6.1 The Counter-fraud and Corruption (CFC) team carries out investigations in all cases of suspected and alleged fraud. They also carry out a proactive programme of fraud awareness, prevention and detection activities designed to minimise TfL's exposure to fraud risk.

6.2 The tenth meeting of the Counter-fraud and Corruption Steering Group was held remotely in Q1. The group discussed a range of subjects including the new 'TfL Security Policy', its associated communications plan and the new TfL 'Security' SharePoint site, which goes live in Q2. Members were provided with an update on the work of the new Chief Information Security Officer is undertaking, which was found to be very informative. The Head of CFC also provided an update to members on the fraud risk reviews taking place with Technology and Data and ongoing significant investigations and CFC team projects.

6.3 A summary of the team's activities during Q1, including information on significant closed fraud investigations, is included as Appendix 10.

6.4 Details of significant new and ongoing fraud investigations during Q1 is included in the paper on Part 2 of the agenda.

7 Resources

7.1 At the beginning of Q1 the Directorate was carrying eight vacancies: Head of Project Assurance, two in Internal Audit, two in Integrated Assurance and three support roles including a data analyst role. There were two leavers: a Senior Risk Manager resigned and an Integrated Assurance Auditor retired.

7.2 There has been a lot of recruitment activity in the quarter with a number of offers being made which will lead to a number of the vacant roles being filled in the next two quarters.

8 Control Environment Trend Indicators

8.1 The Q1 indicators are included as Appendix 11.

List of appendices to this report:

Appendix 1: Level 0 and Level 1 Risks
Appendix 2: Internal Audit reports issued in Q1 2021/22
Appendix 3: Work in Progress at the end of Q1 2021/22
Appendix 4: Work planned for Q2 2021/22
Appendix 5: Cancelled/ deferred/new audits from 2021/22 audit plan
Appendix 6: Internal Audit Q1 summary
Appendix 7: Integrated Assurance Q1 summary
Appendix 8: Project Assurance Q1 summary
Appendix 9: Customer Feedback Q1 summary
Appendix 10: Counter-Fraud and Corruption Q1 summary
Appendix 11: Control Environment Trend Indicators

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

List of Background Papers:

None

Contact Officer: Lorraine Humphrey, Director of Risk and Assurance (Interim)
Email: lorraine.humphrey@tube.tfl.gov.uk