Audit and Assurance Committee

Date: **5 June 2023**

Item: **Risk and Assurance Annual Report and Assurance Statement 2022/23**

This paper will be considered in public

1 Summary

1.1 This is the annual report and assurance statement of the Risk and Assurance Directorate, which comprises of the Enterprise Risk Management, Internal Audit, Quality, Safety and Security Assurance, Project Assurance and Counter-fraud and Corruption teams.

1.2 The Public Sector Internal Audit Standards (PSIAS) requires that the Head of Internal Audit provides an annual Internal Audit opinion based on objective assessment of the framework of risk management, internal control and governance established by TfL management. It is based on a programme of work completed by Risk and Assurance which has been endorsed and monitored by this Committee throughout the year. The assurances in this report are not limited because of a shortfall in resources, absence of skills, limitation of scope or any failure to comply with PSIAS standards overall.

1.3 The opinion can only be reasonable in the sense that no opinion can ever be absolute and reflects the evidence available at the time of drafting. The Internal Audit opinion does not provide any guarantee against material errors, loss, or fraud.

2 Recommendation

2.1 **The Committee is asked to note the report.**

3 Internal Audit Opinion

3.1 In our opinion, TfL's overall framework of governance, risk management and internal control in the year ended 31 March 2023 remains generally adequate for TfL's business needs and operates in an effective manner. However, we draw attention to the following:

(a) our Internal Audit opinion for the year ended 31 March 2022 reported that there had been significant improvements within Procurement and Commercial to improve the control environment. We continue to see improvements in processes and procedures and the implementation of SAP Ariba. There are still gaps in documentation supporting decision making which we identified in the audit 'Use of Consultants and Professional Services, Single Source Requests below £100,000 and Management of

Key Suppliers'. We will conduct follow up work in these areas once the agreed management actions have been implemented and had time to embed; and

(b) the lack of adequate supporting documentation, inconsistent approach to record keeping and document management was a key theme running through our work this year. There is little doubt that resourcing issues have played a part in this with the priority being delivery of services. However, this exposes TfL to possible gaps in its corporate memory and the potential for a lack of transparency and reputational risk. Issues found include but are not limited to:

(i) multiple repositories for storing the same documents with no uniform system in place for managing and maintaining key documents;

(ii) improving the audit trail to support savings made in the Group Portfolio tracking process;

(iii) evidence of decision making when recruiting at executive level, engaging consultants, and professional services;

(iv) documenting assessments of supplier performance; and

(v) records supporting the transfer of assets from TfL to TTL Properties Limited (TTLP)

3.2 We have seen increased support from senior management in closing down management actions in a timelier way, particularly those over 100 days. There is still work to do on closing actions first time and reducing the number of extensions. This should result in improvements in the overall control environment which we will assess in the follow up work we do.

3.3 Concerns over the impact of a lack of employee resource availability has been a consistent theme across all our work. Resourcing levels and their impact on successful delivery, has arisen in a number of Project Assurance and Internal Audit reviews this year. Reviews of resourcing challenges in the commercial and engineering areas show how the situation has developed, however the impact of the introduction of improved resourcing tools and new frameworks has had some positive results.

3.4 The percentage of audit reports given an assurance rating of Poorly Controlled or Requires Improvement has increased from 57 per cent (2021/22) to 76 per cent this year. With audit plans that prioritise risk and core work this increase is not unexpected. It will take at least another annual programme to see if this trend continues and whether this is due to changes in the overall control environment.

Basis of the Internal Audit Opinion

3.5 We are satisfied that sufficient audit and assurance work has been completed to allow us to form a reasonable conclusion on the adequacy and effectiveness of TfL's governance, risk management and control environment.

3.6 The 2022/23 Internal Audit opinion relies on:

(a) the audits carried out by Internal Audit;

(b) the work of the Enterprise Risk team;

(c) project and programme reviews carried out by the Project Assurance team, and third line assurance delivered by Independent Investment Programme Advisory Group (IIPAG);

(d) audits of Safety, Health and Environment (SHE) and Asset Management, and Payment Card Industry Data Security Standard (PCI DSS) reviews carried out by the Quality, Safety and Security Assurance team;

(e) results of any follow up exercises undertaken in respect of previous years' Internal Audit work;

(f) control issues identified by the Counter-fraud and Corruption team in the course of their investigations; and

(g) assurance reviews carried out as part of both the Elizabeth line and TTL Properties Ltd (TTLP) Integrated Assurance Framework.

3.7 Internal Audit (IA) completed 40 internal audits, including those for Elizabeth line and TTLP.

3.8 The Quality, Safety and Security Assurance (QSSA) team completed 90 audits which include Integrated Systems audits, asset quality and compliance with internal or industry standards and PCI DSS compliance audits.

3.9 Project Assurance (PA) have completed 14 programme reviews and 45 project reviews, IIPAG participated in 13 of the programme reviews and 19 project reviews.

3.10 The Counter-fraud and Corruption (CFC) team have managed 21 new cases during 2022/23. The team received 482 miscellaneous referrals.

3.11 An analysis of findings for both IA and QSSA are detailed in Appendix 1.

3.12 There have been no matters arising from any of the work completed that need to be brought to the attention of the Committee.

4 Risk Management

4.1 Understanding and managing risk at all levels within TfL is essential to ensure that we can mitigate the risks as far as is practical and understand our exposure. The Directorate supports the business with Enterprise Risk management at Enterprise (Level 0), Strategic (Level 1) and tactical (Level 2).

4.2 In the past year there has been a significant effort to enhance the effectiveness of Enterprise Risk management in TfL to ensure it remains relevant in our post coronavirus pandemic environment. This work has involved:

(a) reviewing and updating our Enterprise Risks;

(b) ensuring our risk appetite approach is in line with best industry practice and allows more granularity by moving to risk categories. The proposed changes will enable better understanding and engagement with the risk processes and support better decision making;

(c) the Enterprise Risk Management Framework has been updated to align with TfL's Vision and Value Roadmaps. This change enables cross-functional reviews of thematic risks and helps ensure risks are reviewed pan TfL which helps break down silos across the business;

(d) the whole Level 1 process needs to be revamped as historically it was broken down at organisation level. Workshops have taken place, or are in the process of being planned with all Chief Officer areas, with the aim of completing the Level 1 refresh by 31 March 2024 at the latest;

(e) we are now using a single risk tool that allows the direct input of Level 0 and Level 1 risks (previously held on spreadsheets) into the system which therefore provides a single source of the truth for all the three levels of risks. This will give the business better visibility of the risk cascade from enterprise to tactical level; and

(f) consequential changes have also been made to processes and procedures including the Enterprise Risk Assessment Matrix.

4.3 TTLP now has its own Enterprise Risk Framework, linked to TfL's as part of the Integrated Assurance Framework. They have seven Enterprise Risks, and these are being developed with support from the Enterprise Risk team and will be presented to the Land and Property Committee.

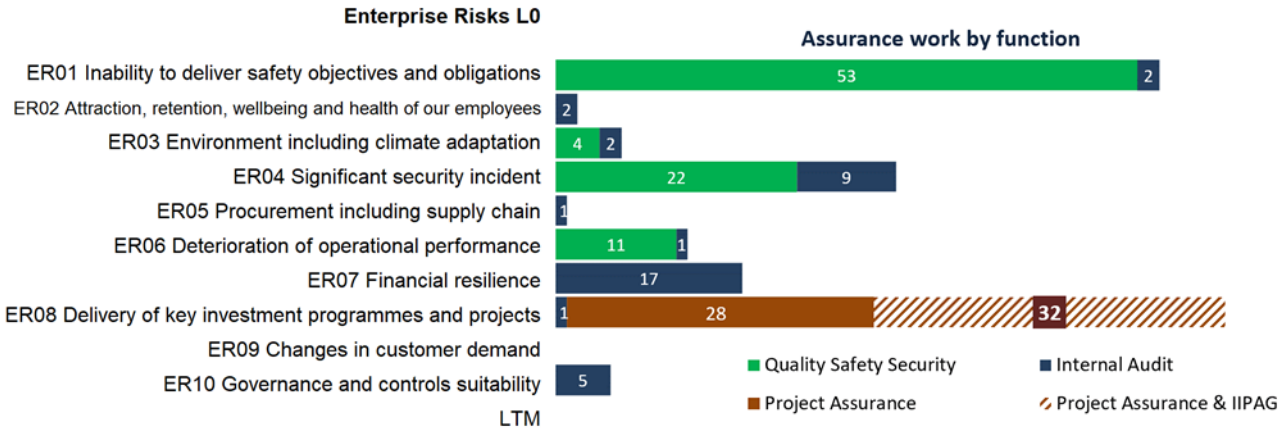
4.4 IA work has shown that risk management at a day to day level is inconsistent in some areas of the business. There were examples where programme wide risk registers were in place but were not regularly reviewed because responsibility for the maintenance and updating of the register had not been assigned as this is a low priority in the business especially where resources are an issue.

4.5 There were two poorly controlled QSSA audits of environmental risk assessments in Buses, Trams and London Underground (LU) which highlighted the risk assessments were incomplete or inadequate. A programme of improvements has now been put in place to complete the assessments and the SHE team have renewed their engagement with operational and maintenance teams on these important risk assessments.

4.6 The CFC team has continued to deliver a range of fraud awareness activities which is designed to prevent and detect fraud and corruption, deter would-be offenders, and educate the workforce about the risk of fraud in the workplace and at home. This includes the hosting of a 'Fraud Awareness week', a digital desktop advertisement about reporting fraud the development and delivery of 'fraud awareness' presentations and workshops to a number of key areas of the business and to support our ongoing collaboration with senior management to prevent and detect financial crime.

4.7 The chart below provides a summary of the work completed at the second and third line of assurance by our various Risk and Assurance teams, by Enterprise Risk. Detailed information of Risk and Assurance work completed against each of the Enterprise Risks is reported quarterly at each Committee meeting.

Figure 1



5 Internal Control

5.1 Effective internal control is essential to ensure that TfL realises its stated aims and objectives. This is achieved through an internal control system that promotes adherence with policies and procedures; the safeguarding of assets; the prevention and detection of fraud and error and the accuracy and completeness of financial and non-financial records. Within Risk and Assurance we look to assess the appropriateness, effectiveness, and compliance with internal controls. Set out below are highlights of key areas of work undertaken this year and issues identified.

Finance and Procurement

5.2 Overall we found that adequate financial controls are in place and operating effectively in Accounts Payable, Fit for the Future Programme, London Transport Museum security of valuable collections and cost verification of the Equans Crossrail Facilities Management contract. The introduction of SAP Ariba in Accounts Payable has improved controls particularly in the registration and maintenance of suppliers. There is now a robust process and control framework in place to support the Group Savings Portfolio tracking process although the audit trail to support savings needed to be strengthened.

5.3 Following the audit of Single Source Requests (SSRs) last year we looked at SSRs below £100,000. It is apparent that the Procurement and Commercial team have made progress in improving the control environment for single source procurements. While we still feel that the number of SSRs is relatively high they represent less than two per cent of the total awarded spend. There are still a number of actions that are nearing completion from previous audits but some of the issues should be addressed with the introduction of SAP Ariba. We will test that and the effectiveness of the implemented management actions as part of our follow up work.

5.4 We continue to provide grant audit certification to the London Transport Museum. This year we certified £508,385 of Arts Council England funding which supports the running of the museum.

5.5 In 2022/23 the CFC team acted on new information received and continued to investigate a number of existing cases related to alleged fraud, corruption, and breaches of TfL policies within the procurement lifecycle. This includes the suspected failure of some TfL employees to disclose conflicts of interest with established suppliers within the supply chain, and allegations of corruption involving a small number of employees and sub-contractors, who have secured work through existing framework agreements with larger Tier 1 suppliers. A number of TfL employees have been subject to disciplinary proceedings and the CFC team has prepared and referred evidence to the British Transport Police Economic Crime team for review and to support criminal investigations and prosecutions.

5.6 The Head of Counter-fraud and Corruption is a member of the newly formed UK Rail Counter-fraud Executive Committee. The Committee is made up of senior fraud specialists from across the rail industry and representatives from the Cabinet Office, Public Sector Fraud Authority, and the Rail Delivery Group. A counter-fraud strategy has been agreed by the Committee and disseminated to all train operating companies who sit on the UK Rail Fraud Forum. Top-level commitment is being sought to collaboratively target high risk and high value fraud types that impact heavily on rail industry each year which will ensure consistent approaches on fraud across the industry.

Safety

5.7 We have seen an improvement in safety assurance this year with the digitising of first line self-assessment tools for the implementation of management system requirements, which should also facilitate greater trend analysis. The QSSA team continue to assess compliance with key Safety Health Environment Management System (SHEMS) requirements across a sample of key operational and maintenance teams, providing actions to the business where legal or internal standards are not met. The SHEMS has been updated and relaunched, at the same time the QSSA team has implemented a new approach to audit planning which means the assurance provided can be directly mapped back to management system components and therefore TfL's strategic risks.

5.8 As a result of the two poorly controlled and one requires improvement audits, QSSA undertook of the compliance with the management system the LU Skills and Development team have embarked on a programme of work to strengthen the competence management systems for all maintenance activities.

5.9 QSSA continue to deliver their programme of short and focused Integrated Systems Audits. Those undertaken in LU Asset Performance and Operational teams tested local compliance with asset specific requirements in addition to critical elements of the management system, including SHE, security, competence, and financial controls. The trends and lessons learnt identified from this work have been well received by management teams.

5.10 IA continued to provide real time assurance on the effectiveness of the procurement process for the development and implementation of a digital SHEMS. The implementation of the new SHEMS has been managed effectively by the project team who have maintained robust review processes throughout.

Environment including climate adaptation

5.11 IA delivered another two audits in the Climate Adaptation series looking at data and reporting. The audit of data found that existing asset data management practices place limitations on embedding adaptation, climate, and weather-related data. Assessing the extent to which existing data can inform and support adaptation has been limited by the lack of easy access to asset data. As a result the improvements to adaptation reporting that remain unaddressed are mainly those that depend upon the recording and availability of comprehensive and consistent adaptation data across operations. The series of Climate Adaptation audits that IA have produced has helped SHE to embed climate change adaptation into existing governance, processes, and internal controls.

5.12 In addition to the two environmental Bus audits mentioned in paragraph 4.5 above, the QSSA team conducted two other environmental audits. One to assess detailed compliance checks against specific requirements of emissions recording for Greenwich Power Station and the other on the programme to manage fluorinated greenhouse gases. Both audits verified that effective controls were in place to meet the specific legal requirements.

Technology and Data

5.13 Technology and Data has been operating with a significant number of vacant posts continuing the theme of resourcing challenge. As a result the audits in this area provide a mixed picture. While half of them were rated as 'Requires Improvement' there was also a lot of good practice identified. Documentation was generally good for SAP Business Planning and Consolidation although the documentation for benefits realisation had not been maintained through the lifecycle of the implementation and beyond. There are good preventive and detective controls for the flows of data between different parts of SAP including daily reconciliations of SAP data. Segregation of duties conflicts for some access controls had been identified and addressed as part of the SAP Business Planning and Consolidation.

5.14 We identified improvements in the way one of our major Information Technology suppliers has taken steps to define procedures and controls in relation to access to their central system. The Revenue Collection contract has the necessary controls in place to comply with the contract. There are regular service review touchpoint meetings and our testing sample confirmed that all joiners, movers and leavers had their access granted, modified and/or revoked in line with TfL and supplier requests.

5.15 We found that the controls for the allocation of strategic and operational ownership of Software Licence Management and the associated governance framework needs improvement. Our review of Data Loss Prevention concluded that overall control could be improved but we confirmed that a range of controls are in place to protect data and reduce the risk of data leakage. Logical access controls are in place to govern data access and encryption controls are operating across the TfL information systems operating environment.

Security

5.16 The assessment of security controls from a second line perspective has resulted in improvements to the management of security risk from project works and the management of Network and Information System assessments in compliance with the regulations. Other areas of work have supported improvement work aimed at improving TfL's security maturity and feasibility reviews of implementing industry standards such as ISO 27001 (Information Security Management Systems).

5.17 QSSA's audits of compliance with the PCI DSS look to ensure that TfL has robust technology, systems, process and competence standards for the processing of card payments. This includes the provision of support and advice to TfL teams introducing new or changing existing payment systems or technology to ensure compliance is designed into the system. Three of these audits were non-compliant, none of which related to processing card data, and work is in hand to achieve compliance.

Counter-fraud and Corruption

5.18 The CFC team has seen an increase in both the new cases managed and the number of new miscellaneous referrals up by 123 per cent on last year. There are several factors behind this increase. There has been increased use of the external fraud reporting tool (through the 'Crime Reporting' page on our TfL website) and, through internal fraud awareness campaigns. There is an increased willingness to report suspected wrongdoing to the team.

6 Governance

6.1 Governance is the combination of processes and structure that the Board puts in place to inform, direct, manage and monitor TfL's activities to ensure the achievement of its objectives. The Risk and Assurance teams look at how this is supported and works in practice at an organisational level. Common findings in audits have included poor records management, clarity over roles and responsibilities and compliance with established procedures. These are essential elements of good governance but can be easily overlooked when the focus is on delivery. To support this the Risk and Assurance leadership team continues to be involved in a range of steering groups and other governance bodies. This involvement enables us to provide input on risk and assurance matters, as well as allowing observation of project and other governance processes.

People

6.2 We found that selection and assessment processes for Executive level recruitment differed in practice to those set out in the pan-TfL Hiring Managers Toolkit. Records of selection decisions, pre-employment checks and vetting were not consistently maintained. We acknowledge that this area has had a high turnover of staff and that senior management accept the identified issues and are acting upon them

Assurance of the Investment Programme

6.3 The primary source of assurance for the delivery of the TfL Investment Programme is through the work of the PA team and IIPAG. PA and IIPAG believe that there is sufficient scrutiny on the Investment Programme in TfL through the various portfolio meetings as well as the Executive Committee Investment sub-group and at the Programmes and Investment Committee.

6.4 Business cases continue to be reviewed in detail where needed in reviews, but still there remains a need to improve the quality of these key documents. There has been positive work undertaken to provide support and improved tools for business case authors, and PA is monitoring the impact of this and supporting the business with these improvement initiatives. There has been a significant focus on ensuring that business cases being submitted to the Department for Transport as part of funding applications meet the required standard.

6.5 IIPAG have produced a number of valuable reports during the year including benchmarking, asset information and asset management, and follow up reviews of progress with improvement programmes within the Procurement and Commercial area and in Programme Management Office.

TTLP Assurance Activity

6.6 In order to ensure there is sufficient assurance around TTLP, a new Integrated Assurance Framework (IAF) was established for the organisation that reports its findings to the Land and Property Committee. The IAF is based on TfL PA, IA and QSSA undertaking risk and assurance activities and a sub-group of IIPAG has been established. An Integrated Assurance and Audit Schedule (IAAS) has been developed and approved by the Land and Property Committee and a number of audits and targeted reviews are underway alongside continuous assurance activities. Good feedback has been provided on the work undertaken to date and the IAAS will be updated as necessary to ensure the IAF continues to be robust.

Security Governance

6.7 In 2021/22 the QSSA team provided support to the Security team in designing and developing the new TfL Security programme which included establishing governance arrangements. The review of security culture maturity in 2022/23 expands upon this work by providing recommendations to the Security team on next steps to enhance security maturity, including governance arrangements.

7 Quality Assurance and Improvement

7.1 In accordance with the PSIAS, IA has an ongoing quality assurance and improvement programme to evaluate our compliance with the Standards and to identify opportunities to improve the effectiveness and efficiency of the function. This is delivered through an annual self-assessment process, but at least every five years we are required to commission an external assessment by a qualified, independent assessor from outside the organisation.

7.2 The Head of IA has now been in post for over a year and the priority has been to deliver the audit plan and reduce the carryover of audits to the following year. This has been achieved and we are now in a position to finalise the review of processes and procedures and implementation of the new IA manual. An internal assessment will be completed in the first half of 2023/24 with the commissioning of a formal External Quality Assessment later in the year.

List of Appendices:

Appendix 1: Analysis of Internal Audit and QSSA findings by category

List of Background Papers:

None

Officer: Lorraine Humphrey, Director of Risk and Assurance
Email: Lorraine.humphrey@tube.tfl.gov.uk

Appendix 1

Analysis of Internal Audit and QSSA findings by category