

**Date: 5 June 2024**

**Item: Risk and Assurance Annual Report and Assurance  
Statement 2023/24**

---

## **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 the Enterprise Risk Management, Internal Audit, Quality, Safety and Security Assurance (QSSA), Project Assurance (PA) and Counter-fraud and Corruption (CFC) 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 2024 remains generally adequate for TfL's business needs and operates in an effective manner. However, we draw attention to the following:
  - (a) the CFC team has identified insider threat as a significant risk to TfL, this spans new and existing employees, non-permanent labour and consultants. Internal audits of recruitment in 2022/23 identified control weaknesses with both recruitment and onboarding processes which were also included in last year's audit opinion. Effective checks are needed on candidate references, supporting information, confirmation of qualifications and vetting of candidates. Improvements are also needed to the documentation that fully supports the decision-making process;

- (b) weaknesses in the controls around the provision of labour contracts have also been identified by the CFC and Internal Audit teams. Additional controls are required to confirm that invoiced labour charges have accurate supporting documentation to ensure that payment is only made for services provided. Discussions are ongoing with the relevant teams to ensure these controls are put in place; and
- (c) while we found improvements in the way supporting information is maintained there are still areas in the organisation where we identified gaps in the audit trail, lack of supporting documentation and an inconsistent approach to record keeping. Our audit of document and records management for procurement and contracts found that records management responsibility was not clearly defined across Procurement and Commercial. There is also no clear view of the procurement documentation held across systems and drives with SAP Ariba not being used for all procurement and contract records. Recommendations were made and accepted around the clarity of guidance, introduction on management checks and communication of the importance of using SAP Ariba as intended.

- 3.2 We continue to be supported by senior management in closing down management actions, particularly those over 100 days. We are seeing an improvement in 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 As part of the Integrated Assurance Framework overseeing Places for London activity has seen improvements in process and investment decisions as the Places for London team respond to the recommendations and actions from targeted assurance reviews and audits. This includes a strengthening of governance arrangements and a review of the property disposal strategy. Over the last year Places for London has focussed on reinforcing their approach to first line assurance through introducing a Programme Management Office function and implementing a project management framework based on TfL's Pathway process.
- 3.4 The percentage of Internal Audit reports given a rating of 'poorly controlled' or 'requires improvement' has decreased from 76 per cent (2022/23) to 62 per cent this year. This is a welcome reduction particularly as the first year of our audit planning prioritising risk and core work saw a significant increase. There has also been a reduction from 24 per cent to 22 per cent in the number of 'poorly controlled' and 'requires improvement' ratings for the QSSA team.

### **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 2023/24 Internal Audit opinion relies on:

- (a) the 43 audits carried out by Internal Audit including those for Places for London;
- (b) the work of the Enterprise Risk team;
- (c) project and programme reviews carried out by the PA team, and the Independent Investment Programme Advisory Group (IIPAG) - PA completed 14 programme reviews and 47 project reviews, IIPAG participated in all of the programme reviews and 21 project reviews;
- (d) the 93 audits of Safety, Health and Environment (SHE), asset quality, and Payment Card Industry Data Security Standard (PCI DSS) audits carried out by the QSSA team;
- (e) results of any follow up exercises undertaken in respect of previous years' Internal Audit work;
- (f) control issues identified by the CFC team in the course of their investigations; 31 new full fraud cases from 985 referrals received and 113 requiring further investigation; and
- (g) assurance reviews carried out as part of the Places for London Integrated Assurance Framework.

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

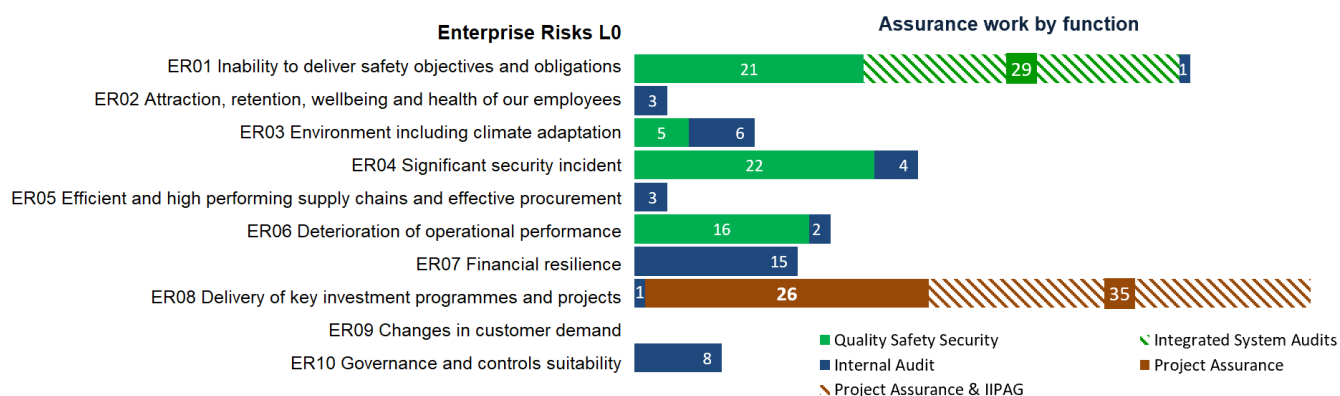
## **4 Risk Management**

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 Risk and Assurance Directorate supports the business with Enterprise Risk management at Enterprise (Level 0), Strategic (Level 1) and tactical (Level 2). Although risk maturity has not been formally measured, we feel that risk maturity is improving. This is as a result of there being greater engagement from the wider organisation. As part of the continuous improvement activity we will also be developing a formal measure in 2024/25 to assess our risk maturity and identify actions required to get us to the 'next level' of maturity. Governance at the Board, Panels and Committees, Executive Committee and its sub-groups is working well with more challenge around items such as risk scores. The quality of the risks is also improving with greater accountability from the owners and responsible managers. Risk appetite has been developed further and we have assigned levels and risk appetite statements developed for each category.

4.2 The Risk Management Policy, procedure and scoring matrix have all been reviewed and updated to reflect changes in the organisational structure and risk management processes.

- 4.3 All the new Enterprise Risks from the last refresh have now been developed and means that all scheduled Level 0 Enterprise Risks have been reviewed by the Executive Committee and the relevant Panels or Committees during the year on a rolling 12 month programme.
- 4.4 Level 1 workshops have been completed for all Vision and Value theme areas and the associated risk development is progressing well. A mapping exercise has been carried out of Level 1s to Level 0s and linkages made in Active Risk Manager (ARM). Engagement has also started with the relevant Executive Committee sub-groups who will have oversight of these risks.
- 4.5 ARM has been configured to include all Level 0 and Level 1 risks alongside the Level 2 risks on one database for the single source of the truth.
- 4.6 Work is in progress to develop Places for London's seven Enterprise Risks which are being presented at the Land and Property Committee. Further work is scheduled to update Places' Enterprise Risk Management Framework and update their Risk Management Plan. Places for London strategic Level 1 risks have been identified using an external consultant and these will be rationalised and included in ARM. The Level 2 will also be input to ARM.
- 4.7 Further work has been undertaken to develop and obtain approval for TfL's new Risk Appetite and Tolerance approach. Risk Appetite Statements have been developed for the agreed risk categories and sub categories based on the agreed risk appetite levels. TfL's risk appetite approach has been reviewed and agreed by the Executive Committee and is supported by the Chair. The information is covered elsewhere on the agenda and then it will be implemented.
- 4.8 Horizon Scanning information highlighting future challenges that may impact TfL's achievement of its objectives is presented to the Executive Committee on a six-monthly basis for discussion and decisions as appropriate.
- 4.9 The CFC team has continued to deliver a range of fraud awareness activities designed to prevent, detect and deter fraud and corruption and educate the workforce about the risk of fraud in the workplace and at home. In 2023/24 the team focused their attention on the insider threat of fraud. This became the theme of annual 'Fraud Awareness week' and all subsequent 'fraud awareness' presentations and workshops to several key areas of the business, where the risk from insider fraud was deemed most significant. This approach supports our ongoing work with senior management to prevent and detect financial crime.
- 4.10 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 - Risk and Assurance Work By Risk By Function



## 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 there are robust financial controls in place and operating effectively in group treasury, accounts receivable, SAP Ariba guided buying, meeting the government funding conditions, journals, Our TfL Programme and the processing of General Data Protection Requirement data by third parties. Some improvement in the control environment was required to the London Transport Museum's financial controls, SAP business expense forms, the headcount controls process and the cost of change. Our audit work continues to demonstrate that TfL has a sound financial control framework.
- 5.3 For the first time we undertook a mid-year review of the TfL Scorecard as there were changes to the metrics and we wanted to identify any potential issues in good time to take remedial action. We found that there were adequate controls in place for the central coordination and local business unit procedures over the collection and processing of data for the purpose of calculating and reporting TfL Scorecard measures. Our end of year audit demonstrated that the findings relating to local processes had been addressed.
- 5.4 Following an IIPAG recommendation to strengthen second line assurance of high value procurements a regime is now in place where focused reviews are undertaken of procurement actions, both the strategic approach and the detailed documentation. Targeted work has been completed on a significant technology project and is ongoing on a framework procurement in the London Underground (LU) Infrastructure area, and a series of new contracts in the Environment Programme. Providing this type of assurance adds value to the procurement process, reducing the risk profile of significant procurements and providing

reassurance to senior management that the processes are robust or that areas of improvement are identified and addressed.

- 5.5 As part of the integrated assurance approach for Places for London Internal Audit has delivered three audits all of which have identified areas for improvement. We found that Places for London needed to complete an end to end review of key processes for new lettings to ensure they are fully documented and remain fit for purpose. We also found gaps in the audit trail for new lettings, the arrangements for revenue and debt collection and the management of property voids with supporting documentation not readily available.
- 5.6 In 2023/24 the CFC team acted on new information received and continued to investigate a number of new and existing cases related to alleged fraud and corruption against TfL and internal breaches of TfL policies. This includes members of the public and some organised criminals targeting the Ultra Low Emission Zone scrappage scheme, allegations of fraud involving a small number of employees and a supplier who falsified attendance and timesheet documents to enable fraudulent payments for ghost labour. Allegations of fraud against TfL employees related to dual working arrangements, obtaining employment using fraudulent references and actively running their own business while on long term sick leave. 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 (BTP) Major, Serious and Organised Crime team for review and to support criminal investigations and prosecutions.
- 5.7 The Head of CFC has continued to collaborate with rail industry leads through membership of the 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. Following the approval of a UK Rail counter-fraud strategy, the Committee and associated UK Rail Fraud Forum (UKRFF) has collaboratively developed a Service Level Agreement with BTP intended to create an agreed level of service and expectation between organisations of the UKRFF, who identify and investigate fraud impacting their organisations, and the uptake and progression of those investigations by the BTP.

## **Safety**

- 5.8 The audit of the safety complaints process found that there are processes in place to manage and handle safety complaints, but these do not always align with the requirements of the safety complaints procedure. We found inconsistencies at an operational level in how the processes were carried out and there was limited evidence to support compliance. There is no doubt that safety complaints are taken seriously but the lack of joined up systems between the teams that deal with them has resulted in more than one single point of failure. All actions have been accepted and are being actioned as a priority.
- 5.9 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 Enterprise Risks.

- 5.10 Following a focus on assurance of LU maintenance teams' competence management systems in 2022/23, there has been a strengthening of the controls as the actions to address causal factors are completed. This has included implementing first line controls and assurance activities, consistency in ways of working and provision of resilience through depth of resource for key competence management roles.
- 5.11 Three audits of the SHEMS identified gaps in the clarity of requirements and roles and responsibilities regarding driving at work, first aid and hazardous substances. These are all subjects that have not been audited previously and the audits have highlighted questions about clarity of roles and responsibilities, as well as the importance of a rolling programme of audits that covers and SHEMS subjects.
- 5.12 QSSA have also delivered their programme of short and focused Integrated Systems Audits in LU Asset Performance and Operational teams. These audits test 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 and show a small improvement in scores (four-six per cent) across all LU Operational teams in 2023/24.

### **Environment**

- 5.13 Internal Audit have delivered a suite of five audits on the impact of extreme weather. Events of extreme weather are predicted to occur with increasing frequency impacting our services, people and assets. TfL's weather plans need to be reviewed and updated to accommodate new information on the hazards and risks of extreme weather events like heavy rain and flooding, heat, wind, snow and ice.
- 5.14 QSSA conducted a follow-up audit of two 2022/23 environmental risk assessment audits on buses, trams and LU which had been rated as 'poorly controlled'. The follow up found that the programme of improvements to complete the assessments had been effective and the 2023/24 audit was rated as 'adequately controlled'.

### **Security**

- 5.15 The telecoms industry will retire analogue telephone networks such as the Public Switched Telephone Network (PSTN) by the end of 2025. TfL has a range of services that are supported by PSTN, both operational and business. Internal Audit examined how this change was to be affected and concluded that the Technology and Data project in place to deliver this was well governed and effectively managed.

- 5.16 TfL has external users, principally suppliers, consultants, non-permanent labour and other third-party delivery partners that may need access to TfL resources such as SharePoint. The TfL sponsor has responsibility for a number of checks prior to requesting access, including due diligence and appropriate level of access. We found that improvements were needed for joiners, movers and leavers and how unused third-party accounts were flagged and deprovisioned.
- 5.17 Internal Audit also looked at the adequacy and effectiveness of the key controls for the accounting and reconciliation of the Revenue Collection Contract transactions. It was apparent that TfL had identified and started to address some of the key reconciliation risks facing the organisation, including data validation and the associated accessibility to appropriate data sources and reporting.
- 5.18 The assessment of security controls from a second line perspective has consisted of a review of the development of security culture maturity within TfL, which identified parts of the policy and management system that need updating and industry good practice that could be adopted within TfL to further maturity in this area. An audit on ransomware risk management determined that Government guidance had been followed, with clearly defined roles and responsibilities and tested by exercise.
- 5.19 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. Six of these 20 audits were non-compliant, none of which related to processing card data. Common issues were maintenance of employee training, asset records and operating procedures, particularly during personnel or organisational change. These issues have been easily and swiftly resolved and highlight the importance of this regime of annual assurance of these controls.

## **Counter-fraud and Corruption**

- 5.20 The CFC team has seen an increase in both the new cases managed and the number of new referrals. In 2023/24 referrals increased to 985 with 31 new full fraud cases under investigation. This compared to 482 referrals and 21 new full fraud cases in 2022/23. There are several factors behind this increase. Use of the external fraud reporting tool (through the 'Crime Reporting' page on our TfL website) continues to increase, likely due to social media fraud awareness messaging. There continues to be an increased willingness to report suspected wrongdoing to the team, which is a good thing.

## **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, lack of clarity over roles and responsibilities and compliance with established procedures which are essential elements of good governance. To support this the Risk and Assurance leadership



team continues to be involved in a range of steering groups and other governance forums. This involvement enables us to provide input on risk and assurance matters, as well as allowing observation of project and other governance processes.

- 6.2 We found that there are robust governance arrangements for the TfL pension fund trustee board, the national rail reimbursement scheme and reporting the TfL Scorecard results. The gifts and hospitality policy and procedure is well established but overall compliance needs to be embedded across the organisation with TfL advisory groups being included in reporting. We recommended that the scope of the gifts and hospitality policy requires review to ensure that all are included.

### **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 Project Assurance (PA) team and IIPAG. PA and IIPAG believe that there is sufficient scrutiny of 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 quality of these key documents continues to be quite variable and multiple improvement recommendations have been made this year although improved support and tools have provided some benefit. There has been a significant increase in activity relating to business cases being prepared for submission to the Department for Transport as part of funding applications. Extensive assurance support has been provided to ensure that the documents meet the required standards and the feedback has been positive from the Department for Transport.
- 6.5 IIPAG has produced a number of reports during the year including a review of the delivery of infrastructure renewals, the effectiveness of TfL's Pathway project stage gate process, and their annual review of the first and second lines of assurance. In addition, a progress review was undertaken to review progress in the undertaking of actions from an earlier review of an improvement programme in the Procurement and Commercial area.

### **Places for London Assurance Activity**

- 6.6 The Places for London Integrated Assurance Framework is based on a Three Lines of Assurance model. Line one, management functions of Places for London and key interfaces; line 2, PA and QSSA; line three Internal Audit and a sub-group of IIPAG.
- 6.7 PA undertook a number of targeted assurance reviews including resourcing, procurement and commercial arrangements, and Places for London governance. PA provide continuous assurance of major developments within the property development portfolio and other significant investment programmes. IIPAG, supported by PA have completed reviews of retail strategy, joint venture management, residential strategy and property disposal strategy.

- 6.8 QSSA completed a Health and Safety audit of tenancy compliance. In parallel Internal Audit completed audits on property transfer accounting; accounting and cash management process; revenue collection and debt management; and due diligence process for new tenants.
- 6.9 Recent activities have focused on strengthening continuous second and third-line assurance activities with a PA and IIPAG representative being assigned to each Places business sector. This has strengthened relationships and further improved the assurance team's understanding for the Places business.

## **7 Quality Assurance and Improvement**

- 7.1 In accordance with the PSIAS, Internal Audit has an ongoing quality assurance and improvement programme to evaluate compliance with the Standards and to identify opportunities to improve the effectiveness and efficiency of the function. In preparation for an External Quality Assessment planned later in 2024 and internal assessment has been completed. This identified some areas for improvement and these will be addressed along with a comprehensive review and update of our working papers and processes. The Institute of Internal Auditors has also agreed new audit standards which will be effective from January 2025. How these effect our work will also be included in the review.

### **List of Appendices:**

None

### **List of Background Papers:**

None

Officer: Lorraine Humphrey, Director of Risk and Assurance  
Email: [Lorraine.humphrey@tube.tfl.gov.uk](mailto:Lorraine.humphrey@tube.tfl.gov.uk)