Appendix 1 – Quality, Safety and Security Assurance Audits Completed in Quarter 4 of 2022/23

ER1 Inability to deliver safety objectives and obligations

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Asset Performance Delivery	22 791	London Underground (LU) Test Train Operators Competence Management	To assess the competence management system compliance with Office of Rail and Road Guidance and internal standards	Adequately Controlled	The majority of the requirements of the LU Competency Management System have been satisfied. There were some elements that need strengthening.
TTLP	22 784	TTL Properties Limited (TTLP) Property Management: Assurance of tenants safety compliance	To seek assurance that tenants statutory and contractual compliance with health and safety requirements is being assured by the TTLP Property Management team.	Adequately Controlled	The Compliance team were assured of tenants' compliance through a managed inspection programme. The assurance of fire risk assessments has improved as a result
Engineering and Asset Strategy	22 735	Management of Engineering Safety Critical Licensing	To provide assurance that engineering employees undertaking safety critical tasks are suitably managed in accordance with legislation and TfL Standards.	Requires Improvement	There were a few non-conformances with key requirements of the management system, notably recording hours of work, identifying safety critical workers in SAP, communicating working time limits and implementation of a drug and alcohol testing regime.
Project & Programme Delivery	22 768	Capital Delivery Systems Management of CDM Principal Designer duties in Asset Renewals Programme	To seek assurance that Principal Designer roles responsibilities for the Structures and Major Asset Renewal Programmes projects are being appropriately allocated and documented in keeping with the Construction (Design and Management) Regulations, Guidance and TfL Standards.	Requires Improvement	Whilst there was satisfactory evidence of Client and Principal Designer engagement, formal documents relating to assessment and appointment of Principal Designers were not sufficiently evidenced. Improvements to the current procedures and SHE and Project Manager engagement are required

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Rail & Sponsored Services	22 765	DLR Annual Safety Audit - Worksite Access, Method Statements and Fire Management	To provide assurance that the DLR Management System is compliant across a sample of critical business processes	Requires Improvement	A number of non-conformances in relation to the fire management and Temporary Approved Non-Compliances requirements were identified.
Asset Performance Delivery	22 763	LU BCV/SSL Institution of Railway Signal Engineers (IRSE) Signalling Competence	Annual audit of LU IRSE Agency for compliance to IRSE requirements	Well Controlled	The requirements of the IRSE standard for competence of signalling staff were fully evidenced.
Rail & Sponsored Services	22 767	London Overground (LO) change management - infrastructure maintenance	To provide assurance that the revised LO change assurance process has been successfully implemented and is operating effectively for infrastructure changes.	Well Controlled	LO was found to be managing and controlling the infrastructure management change process in accordance with the revised procedure. Significant improvements have been made to ensure compliance.

Integrated Systems Audits

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Asset Performance Delivery	22 775	Cockfosters Fleet Depot Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	76.6 per cent conformance, 49 green, 2 amber 13 red (compliant, minor non-conformance, major non-compliance)
Asset Performance Delivery	22 774	Northern Track Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	51 per cent Conformance, 23 Green, 6 Amber, 16 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	22 781	Stratford Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	69.6 per cent conformance, 39 Green, 0 Amber, 17 Red (compliant, minor non-compliance, major non-compliance)

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Customer Operations - LU	22 801	LU Brixton Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	57 per cent Conformance, 32 Green, 0 Amber, 24 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	22 800	LU Neasden Traincrew Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	40 per cent conformance, 14 Green, 00 Amber, 21 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	22 799	LU Kilburn Park Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	72 per cent Conformance, 41 Green, 0 Amber, 16 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	22 798	LU Warren Street Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	67 per cent Conformance, 37 Green, 1 Amber, 18 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	22 797	LU Hammersmith Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	47 per cent Conformance, 27 Green, 2 Amber, 28 Red (compliant, minor non-compliance, major non-compliance)

ER4 Significant security incident

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Customer Operations - LU	22 746	Payment Card Industry Data Security Standards (PCI DSS) Compliance: CPAY Pin Entry Devices (PEDs)	To seek assurance that the CPAY PEDs within the Ticket Vending Machines on the LU stations are operating in compliance with the PCI DSS and additionally TfL's contractual obligations to its Acquiring Bank.	Adequately Controlled	Contactless PEDs were found to be compliant to the PCI DSS. The PED devices are implemented and maintained within a secure PCI Point to Point Encrypted environment.

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
London Transport Museum (LTM)	22 787	Payment Card Industry Data Security Standard Compliance Audit: London Transport Museum Friends (Chip & PIN)	To seek assurance that LTM Friends is operating in compliance with the PCI DSSv.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The 'Friends of the LTM' (Chip and PIN Machine) was found to be compliant to the PCI DSS.
Rail & Sponsored Services	22 757	Payment Card Industry Data Security Standard Compliance Audit: London Cable Car	To seek assurance that the London Cable Car is operating in compliance with the PCI DSSv.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The IFS Cloud Cable Car was found to be compliant to the PCI DSS.
Technology & Data	22 786	Payment Card Industry Data Security Standard Compliance Audit: CPAY (Pass Agents)	To seek assurance that the Pass Agents team is operating in compliance with the PCI DSS and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The Pass Agents/ Bulk Sales was found to be compliant to the PCI DSS.
TTLP	22 758	Payment Card Industry Data Security Compliance Audit: TfL Film Office	To seek assurance that the Film Office is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The TfL Film Office was found to be compliant to the PCI DSS. There are no observations raised and no management actions required.

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Chief Finance Officer	22 789	Payment Card Industry Data Security Standard Compliance Audit: Financial Services Centre(FSC)	To seek assurance that controls and systems are in place that meet the requirements of the PCI DSS.	Adequately Controlled	The FSC was found to be compliant to the PCI DSS.
Chief Customer and Strategy Officer	22 788	Payment Card Industry Data Security Standard Compliance Audit: Lost Property Office (LPO)	To seek assurance that controls and systems are in place that meet the requirements of the PCI DSS.	Adequately Controlled	The LPO was found to be compliant to the PCI DSS. There was one management action raised.
Pan TfL	22 734	Consultancy: ISO 27001 Distance to Go Audit	To provide consultancy services on how closely TfL's Cyber Security team's management of cyber security risk is aligned to ISO 27001 and what key activities would be required to meet the standard.	Memo	The review addressed key elements of the management system required to meet the requirements of ISO27001. Each of these elements is addressed in turn by a separate section in the report. A conclusion is provided at the end of each section indicating what clauses of ISO27001 apply and whether the associated requirements are ‘Met’, ‘Partially met’ or ‘Not met’. A list of recommendations has been provided to the management team.
Rail & Sponsored Services	22 803 U	Payment Card Industry Data Security Standards Compliance Audit: London Cycle Hire Front End	To seek assurance that London Cycle Hire Scheme (LCHS) is operating in compliance with the PCI DSSv3.2.1 and additionally TfLs contractual obligations to its Acquiring Banks	Requires Improvement	Cardholder data is processed by TfL and Service Provider staff in a secure and compliant manner however, further work is required to strengthen the required controls to address the security risk assessment process as applicable to PCI DSS.
Technology & Data	22 756	Payment Card Industry Data Security Standards Compliance Audit: Visitor Centre (TOMs)	To seek assurance that the Visitor Centres (VC) is operation in compliance with the PCI DSS and additionally TfL's contractual obligations to its Acquiring Banks.	Requires Improvement	Cardholder data is processed by TfL VC staff in a secure and compliant manner however, the Service Provider has not maintained the device asset register.

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Technology & Data	22 785	Payment Card Industry Data Security Standard Compliance Audit: CPAY (mobile apps and website)	To seek assurance that the TfL Website and Mobile Apps are operating in compliance with the PCI DSSv.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	Requires Improvement	The mobile app, customer contact centres and website payment channels were found to be compliant to the PCI DSS. However, further work is required to address the findings from the September 2022 'Contactless (CPAY) and LCHS PCI DSS Backend Assessment'.

ER6 Deterioration of operational performance

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Asset Performance Delivery	22 736	Thales Jubilee and Northern Lines Signal Design Authority Services	To seek assurance that design authority services are provided by Thales in accordance with the Technical Support and Spares supply Agreement (TSSSA)	Not Rated	The core elements of this amended contract are being fulfilled. The Design Authority service requirements are relatively new, (TSSSA Amendment 2022) and the service delivery and TfL expectations are in the process of being aligned. Many of the issues relate to harmonisation of processes operated by each party with a view to improving overall service delivery.
Asset Performance Delivery	22 730	Management of Civil Engineering Deep Tube Project Asset Data for New Assets	To seek assurance that deep Tube civil engineering asset data is being actively identified and recorded in the asset database, for new assets	Poorly Controlled	The management arrangements for registering new assets were not working effectively. This prevented new assets being inspected within the timescales defined by engineering standards.

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Asset Performance Delivery	22 733	Removal of PCB Containing Components	To seek assurance that the removal of Polychlorinated Biphenyls (PCB) components is being undertaken as agreed with the Environment Agency.	Adequately Controlled	Adequately controlled - The PCB removal programmes were found to be adequately managed by the comms, power, fleet, signals and SHE environment teams with a target to be PCB free by end of 2023. Progress is reported quarterly to the Environmental Agency by TfL SHE Environment team.
Rail & Sponsored Services	22 721	Handover of Tram Fleet Asset Information from Projects to Maintenance Teams	To follow up on previous 'Poorly Controlled' conclusion audit - To seek assurance that asset data is routinely updated following changes to Tram fleet assets to ensure they can be maintained	Requires Improvement	There have been some improvements since the 20 724 audit with the management of risks, reporting, and maintenance of master document lists. There were non-conformances raised with the Pathway Stage Gate process which were raised in the 20 724 audit, and the provision of records for maintenance instructions, training and equipment.
Rail & Sponsored Services	22 772	DLR Rolling Stock Maintenance Compliance: B92, B2007 and Engineering Vehicles	To provide assurance that DLR rolling stock vehicles are being maintained in accordance with engineering standards with the correct records maintained regarding people, plant and process.	Well Controlled	All of the areas reviewed during the audit met the requirements of the standards. A robust and well managed approach to the maintenance of DLR rolling stock was evident throughout