Appendix 1 – Quality, Safety and Security Assurance Audits Completed in Quarter 4 of 2021/22 against ER1, ER4 and ER12

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER01 Major health, safety or environmental incident or crisis	London Overground (LO)	21 730	London Overground Safety Authorisation	To provide assurance that LO is complying with its Safety Authorisation document including safety, risk, competency, and infrastructure protection.	RI	– It could not be demonstrated that safety responsibilities of staff with key safety posts had been documented, a medium priority finding was raised. The controls tested within Infrastructure Protection and Competency Management were found to be working effectively.
	LU Asset Operations	21 760	LU Railway Engineering Works and Track Modification Unit Competence Management	To assess the effectiveness of and compliance with arrangements designed to ensure tasks are completed competently	RI	Critical areas of procedure PR0694 A3, Workshops: Training and Development and supporting documentation had not been fully implemented, which affects compliance with Office of Road and Rail guidance on competence management systems
	Surface Project and Programme Delivery	21 761	Surface Programme and Project Directorate Structures Design and Construction Compliance	To examine how it is assured that construction complies with approved designs and quality requirements	RI	Some key Construction, Design, Management (CDM) and quality documentation including completed Testing and Inspection, Compliance Certificates and Health and Safety File information was either not available or had not been approved within defined timescales
	Pan-TfL	21 759	TfL Lone Working	To seek assurance that management arrangements for lone working are effective at ensuring legal compliance and protecting the safety and wellbeing of TfL employees	RI	Requires Improvement - Management System content on lone working activities did not fully reflect the current Health, Safety and Environment (HSE) guidance (INDG 73). Training elements identified as risk assessment control measures had not been fully implemented.
	Commercial Development	21 739	Commercial Development Commercial Property HSE Compliance	To seek assurance that the Commercial Property Team are SHE compliant.	AC	Adequately Controlled - Compliant and proportionate risk control processes were evidenced in the HSE areas reviewed, with the exception of staff Work Risk Assessments , which are being addressed on an action plan.

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER01 Major health, safety or environmental incident or crisis	Network Management	21 752	Surface Transport Fire Risk Assessments (FRA)	To provide assurance that appropriate FRA assessments and fire strategies are in place for all direct managed Surface Premises (Bus, Victoria Coach Station, River, Dial a Ride and Ferry).	AC	Fire Risk Assessments were mostly found to be completed correctly and described in a draft ST Procedure; this document describes the fire safety arrangements of ST Asset Operations (AO) but has not been formally agreed. It is a requirement of the Regulatory Reform (Fire Safety) Order 2005 that fire safety arrangements are documented.
	Rail and Sponsored Services	21 755	Docklands Light Railway (DLR) Rolling Stock Plant and Equipment Management	To examine the management of rolling stock plant and equipment in line with statutory requirements by Keolis Amey Docklands (KAD)	AC	Adequately Controlled – The vast majority of servicing and maintenance of Rolling Stock Plant and Equipment meets the requirements of Maintenance Manual (Rolling Stock) Rolling Stock and Depot Maintenance Procedure EN-RS-MP-701-G Issued 26/07/2016
	Rail and Sponsored Services	21 758	DLR Safety Management	Annual Audit required by DLR's Safety Authorisation to assess compliance with a sample of joint business critical processes. The focus will be on the management of changes, with workplace risk assessments as a secondary element.	AC	The written arrangements for managing change and workplace risk assessments were seen to be implemented effectively
	Rail and Sponsored Services	21 765	DLR Lifts and Escalators Asset Management	To assess compliance with the Lifting Operations and Lifting Equipment Regulations and Safety (Workplace) Regulations	WC	Legislative requirements for statutory inspections of Lifts and Escalators were complied with.
	LU Asset Performance and Capital Programmes	21 811	Greenwich Power Station Greenhouse Gas Monitoring	To assess effectiveness of Greenwich Generating Station's arrangements for data monitoring and reporting of Carbon dioxide emissions for the UK Emissions Trading Scheme .	WC	There is no cause for concern, the controls are well designed and implemented. There is one low priority finding raised to enhance the existing record retention process.
	LU Asset Performance and Capital Programmes	21 813	Institution of Railway Signal Engineers (IRSE) Licensing	To assess signals Bakeloo, Central, Victoria and Su-Surface lines against the IRSE competence requirements	WC	The requirements of the IRSE standard for competence of signalling staff was seen to be fully met

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER04 Major security incident	Strategy & Chief Technology Officer	21 777	Consultancy: New Ticketing Card Reader Systems	To provide consultancy services that advise duty holders on the implementation of the requirements of the Payment Card Industry Data Security Standards (PCI DSS)	Memo	The details of the penetration testing phase can be found in a separate report due it's sensitivity classification. The content of this report consists of a summary of the findings from the penetration testing phase and the detailed findings of the physical security review phase.
	Surface Transport, Network Management	21 803	Network Information Systems Regulation compliance: ST Tunnels and SCADA	To provide assurance that local systems are compliant with the requirements of the NIS Regulations and the Cyber Assessment Framework (CAF)	AC	The Tunnels closed circuit television and SCADA CAF and Service Improvement Plan (SIP) documents have been agreed and submitted to the Department for Transport (DfT). An improvement activity plan is well underway.
	TfL Engineering and Asset Strategy	21 802	Network Information Systems Regulation Compliance: LU Power	To seek assurance that TfL is meeting it's obligations under the DfT NIS Regulations regarding the management of a framework of assessments.	AC	The LU Power Cyber Assurance Framework (CAF) and System Improvement Plan (SIP) documents have been agreed and submitted to the DfT. An improvement activity plan is well underway.
	Surface Transport	21 801	Network Information Systems Regulation Compliance: ST Urban Traffic Control	To seek assurance that TfL is meeting it's obligations under the DfT NIS Regulations regarding the management of a framework of assessments.	AC	Urban Traffic Control were selected as a sample of TfL Network and Information Systems performance. The UTC Cyber Assurance Framework (CAF) and Service Improvement Plan (SIP) documents have been agreed and submitted to the Department for Transport (DfT). An improvement activity plan is well underway.
	Strategy & Chief Technology Officer	21 799	Network Information Systems Regulation Compliance: LU Connect	To provide assurance that local systems are compliant with the requirements of the NIS Regulations and the Cyber Assessment Framework (CAF)	AC	Connect was selected as a sample of TfL NIS Regulations performance. The Connect Cyber Assurance Framework and Service Improvement Plan documents have been agreed and submitted to the Department for Transport.

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER04 Major security incident	Surface Transport, Rail and Sponsored Services	21 796	London Overground Local assessment of Network Information Systems Regulation compliance	To provide assurance that the security risks relevant to the TfL Operational Technology systems are managed in an effective manner that ensures the integrity and resilience of these systems in meeting the obligations under the DfT (NIS) Regulations.	RI	London Overground (LO) Management and Cyber Security Teams requested this audit to assist in the completion of their Cyber Assessment Framework (CAF). The CAF is currently in draft with specific cyber security gaps.
	LU Asset Performance and Capital Programmes	21 795	Payment Card Industry Data Security Standards Compliance Audit: NPS	To seek assurance that the Network Planning and Services (NPS) Plant and Materials is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	The NPS is compliant to the PCI DSS.
	Surface Transport, Bus Operations	21 794	Payment Card Industry Data Security Standards Compliance Audit: Bus Stop Closures	To seek assurance that the Bus Stop Closure is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	Bus Stop Closures team was found to be compliant to the PCI DSS.
	Surface Transport, Bus Operations	21 793	Payment Card Industry Data Security Standards Compliance Audit: Victoria Coach Station (VCS)	To seek assurance that the VCS is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	The VCS was found to be compliant to the PCI DSS. There is one action required: to complete the PCI DSS awareness training for applicable staff.
	Strategy & Chief Technology Officer	21 792	Payment Card Industry Data Security Standards Compliance Audit: Art on the Underground (AOU)	To seek assurance that the AOU is operating in compliance with the PCI DSS v.3.2.1 and TfL's contractual obligations to its Acquiring Banks.	AC	Compliant. Due to the ongoing COVID-19 pandemic Art On Underground has been working remotely since March 2020 and have not had an occasion to use the payment card machine which remains securely stored within the office.

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER04 Major security incident	Strategy & Chief Technology Officer	21 790	Payment Card Industry Data Security Standards Compliance Audit: Staff Travel	To seek assurance that the Staff Travel is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	The Staff Travel team is compliant to the (PCI DSS).
	Strategy & Chief Technology Officer	21 789	Payment Card Industry Data Security Standards Compliance Audit: Lost Property Office (LPO)	To seek assurance that the LPO is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	The Lost Property Office (LPO) was found to be compliant to the PCI DSS. There are no management actions required.
	Strategy & Chief Technology Officer, London Transport Museum	21 787	Payment Card Industry Data Security Standards Compliance Audit: London Transport Museum Friends (Chip & PIN)	To seek assurance that the Friends of LTM is operating in compliance with the PCI DSS v.3.2.1 and additionally TfL's contractual obligations to its Acquiring Banks.	AC	The Friends of London Transport Museum (LTM) was found to be compliant to the PCI DSS. There are three recommendations that are required in preparation for the return to office and pre-pandemic operations.
	Strategy & Chief Technology Officer	21 783	Payment Card Industry Data Security Standards Compliance Audit: Mobile and Website	To seek assurance that controls and systems are in place that meet the requirements of the PCI DSS for the TfL Website, Mobile Apps and Contact Centre Operations.	AC	The mobile phone applications, telephone contact centres and website payment channels were found to be compliant to the PCI DSS. There is further work to be undertaken on strengthening the security controls and addressing the findings from the security penetration test review performed by a specialist security partner.
	Strategy & Chief Technology Officer	21 781	Payment Card Industry Data Security Standards Compliance Audit: Financial Services Centre(FSC)	To seek assurance that controls and systems are in place that meet the requirements of the PCI DSS	AC	The FSC was found to be compliant to the PCI DSS

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER12 Asset condition unable to support TfL outcomes	LU Asset Performance and Capital Programmes	21 754	LU Management of Faults	To provide assurance that changes to the management of faults have been effective and are suitably used to manage the performance of the maintainer/supplier	AC	The lessons learnt from the Kentish Town Formal Investigation Report regards monitoring and escalating overdue faults have been implemented. Work was in progress to review legacy faults from Ellipse that currently have no associated work orders.
	LU Asset Performance and Capital Programmes	21 774	LU Osterley Step Free Access Project Design and Construction	To examine Pathway compliance to ensure that the development of design and construction to the design ensures safety and technical compliance	RI	The audit identified opportunities to enhance assurance of the Principal Contractor's arrangements. Additionally, not all formal mechanisms to record non-conformances and recording lessons learnt were utilised
	LU Asset Performance and Capital Programmes	21 762	Management of Rail Grinders	To follow up previously raised issues on rail grinding. Also to assess conformance to TfL standards documents when operating and maintaining rail grinders.	RI	Requires Improvement – Medium and low priority issues were raised relating to documentation on the use and approval of the rail grinding machines. This raises the risk that some assurance for the safe operation of the machines is not in place.

Integrated Systems Audits

Enterprise Risk	Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
ER01 Major health, safety or environmental incident or crisis	LU Customer Operations	21 710	Hampstead Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	Conformance Rate = 78%. Significant issues related to workplace risk assessments not being available, presumed expired, missed inspections, no defined inspection checklist, secure room training, Lift communication checks, Station Information Files, weekly emergency equipment checks, fire drill records at one station, auditable records of rule book change communication, registers for controlled ticketing and revenue stationary.
ER01 Major health, safety or environmental incident or crisis	LU Customer Operations	21 714	Wembley Central Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	Conformance rate = 69.5%. Significant issues related to medical restriction risk assessments, lone working, systems checks, inspection checklists, inspections of secure rooms, in-cab monitor checks, lift communications checks, COVID-19 assurance checks, Local Station Information Files reviews, staff and tenants familiarisation, fire control panel checks, quarterly financial systems checks
ER01 Major health, safety or environmental incident or crisis	LU Customer Operations	21 716	Hainault and Wanstead Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	Conformance Rate = 65% Significant issues related to medically restricted risk assessments, buddy calls for lone working, inspection checklist, completion of inspections including in secure rooms, lift inspections, COVID-19 inspections, Station Information File reviews, checking of track layout diagrams, fire risk assessment actions and familiarisations, Security plans, security checks, expired competence plans, night worker health questionnaires, communication of rule book changes, completion of financial system checks, control of ticketing and revenue controlled stationary

ER01 Major health, safety or environmental incident or crisis	LU Customer Operations	21724	Brixton Traincrew Operations Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	Conformance rate of 68% Significant issues related to risk assessments for computers use and medically restricted staff, inspection checklist, fire risk assessment actions, fire drills, checking of track circuit diagrams and other emergency equipment, health questionnaires for night workers, weekly payroll audits
ER01 Major health, safety or environmental incident or crisis	LU Asset Performance and Capital Programmes	21728	BCV Signals Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	Conformance Rate 56% - Significant issues related to substances hazardous to health, computer use, actions from risk assessments, medical restriction risk assessments, review of live working justifications, COVID-19 assurance checks, night worker health questionnaires, training for working at height and manual handling, approved driver training and vehicle checks, working at height equipment checks, fire drills, weekly fire equipment tests, first aid arrangements, storage of non-useable equipment, Temporary Approved Non-Compliance Accountable Person competence maintenance
ER01 Major health, safety or environmental incident or crisis	LU Asset Performance and Capital Programmes	21766	LU Power and Electrical - Cables Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	conformance rate = 76%. Significant issues related to workplace risk assessments, substances hazardous to health assessments, computer use assessments, COVID-19 assurance checks, tracking safety critical licences, tracking of manual handling and working at height training, inspection of ladders, Temporary Approved Non-Compliance work not completed on time, signing off of work orders by appropriate manager