Safety, Sustainability and Human Resource Panel

Date: **15 November 2023**

Item: **Safety, Health and Environment Assurance Report**

This paper will be considered in public

1 Summary

1.1 The purpose of this report is to give the Panel an overview of the effectiveness of the risk controls for Enterprise Risk 1 (ER1) – 'Inability to deliver safety objectives and obligations', Enterprise Risk 3 (ER3) – 'Environment including climate adaptation' based on second line of defence audit work by the Quality, Safety and Security Assurance (QSSA) team and third line of defence work by the Internal Audit team. Information is also provided on Enterprise Risk 6 (ER6) – 'Deterioration of operational performance' and Enterprise Risk 4 (ER4) – 'Significant security incident including cyber security' as they correlate to ER1.

1.2 As of Quarter 2 of 2023/24 (25 June to 16 September 2023) (Q2) all QSSA audits have been planned and conclusions recorded against the applicable management system document. It is too early for analysis of results as a relatively small proportion of the management system has been covered in 2 quarters, but the audit planning stage has identified historical gaps in assurance and resulted in more comprehensive audits that address whole management system procedures. This indicates that the change of approach is working as we intended.

1.3 Appendix 1 provides a list of applicable audits undertaken in Q2. Audit reports issued are given a conclusion of 'well controlled', 'adequately controlled', 'requires improvement' or 'poorly controlled'. Individual findings within audit reports are rated as high, medium or low priority.

1.4 Performance data is provided on progress against the audit plan, audit ratings, rating trends by Enterprise Risk and business unit and progress against actions, with comparisons provided across the last two years.

2 Recommendation

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

3 Annual Quality, Safety and Security Assurance Audit Plan

3.1 The annual QSSA audit plan contains a series of second line of defence audits that address ER1, ER3, ER4 and ER6.

3.2 The 2023/24 audit plan was revised at the end of Q2 to ensure the proposed audits for Quarters 3 and 4 still reflect concerns of the business and assurance needs. This involved consultation with risk and management system owners from Safety, Health and Environment (SHE), Operations, Maintenance, Engineering Directorates and Security teams. Each audit has an identified sponsor within TfL to whom assurance is provided, typically a management system or risk owner or a TfL assurance team.

4 Work of Note this Quarter

4.1 ER1 and ER4 have both been reviewed and updated in Q2, with revisions made to the scope and risk ratings. An update on ER1 is included on the agenda for this meeting and ER4 is scheduled to be reviewed at the 29 November 2023 Audit and Assurance Committee meeting. There have been no changes of note to the causes, controls or ratings of ER3 and ER6 in Q2. ER6 will be revised in Quarter 3 following internal workshops.

4.2 Internal Audit issued one report against ER3 in Q2: 'Climate Adaptation - risk assessments' issued as a memo. Three other audits are in progress: 'Impact of Extreme Weather-Heavy Rain and Flooding' and 'Impact of Extreme Weather-Heat' both under ER3 and 'Safety Complaints Process' against ER1.

4.3 A total of 19 second line QSSA audits were delivered in Q2, taking the total to 67 per cent of the Quarter 1 (1 April to 24 June 2023) (Q1) and Q2 plan for 2023/24 (see Appendix 1 for the full detail of audits completed in Q2). This is slightly behind target but considered recoverable within the next two quarters.

4.4 Four audits were concluded as 'requires improvement', all have agreed and tracked action plans in place:

(a) London Underground (LU) Management of Lift and Escalator Incidents: elements of the associated procedure PR0775 did not fully reflect current practices and requires updating to ensure there is a consistent understanding amongst stakeholders of key definitions and decision points following an incident.

(b) Trams Incidents and Accidents Process Compliance: There was evidence of good communication between TfL and Trams Operations Limited regarding significant incidents. Some requirements of the procedure were not sufficiently evidenced and are the focus of the agreed actions.

(c) Payment Card Industry Data Security Standard (PCI DSS) Compliance Audit: TfL and London Transport Museum Operations Centre: Employee training was out of date and key manuals needed updating to reflect recent changes to the ticketing systems in use.

(d) PCI DSS Compliance Audit: TfL and London Transport Museum Shop. The documentation regarding staff training and asset data was out of date and missing key information.

4.5 Six audits were concluded as 'adequately controlled' and two audits were concluded as 'well controlled' along with six Integrated Systems audits which are not rated as they cover multiple subjects and risks.

4.6 The breakdown of the audits completed in Q2 by risk is as follows:

(a) 10 audits were completed against ER1: six of which were Integrated Systems audits of LU, two were ‘requires improvement’, one was ‘adequately controlled’ and one was ‘well controlled’;

(b) six audits were completed against ER4 all of which were PCI DSS compliance audits: four of which were ‘adequately controlled’ and two were ‘requires improvement’; and

(c) three audits were completed against ER6 and were concluded as ‘well controlled’, ‘adequately controlled’ and a memo.

4.7 QSSA has begun a series of internal reviews against ISO 55000 Asset Management as a gap analysis. The reviews are at the request of TfL Engineering to provide localised and overall findings against the ISO standard as a measure of good practice. The reviews will also be used to inform any future decisions regarding application of the standard. The first review has been completed within London Overground and has provided recommendations for further action structured around the standard. Further reviews are scheduled for the remainder of the year.

5 Cancelled and Deferred Work

5.1 All cancellations and deferrals are undertaken in consultation with the sponsor. Two audits were cancelled in Q2:

(a) Consultancy: TfL Control of Track Access. This was cancelled as a SHE ‘deep dive’ is currently taking place on this subject which will make recommendations to improve control; and

(b) Supplier Assurance: Compliance with LU Fire Standards. This was cancelled as the contract is being revised, introducing new requirements which will require assurance at a later date.

5.2 Two audits were deferred to next year’s audit plan:

(a) Rail for London Infrastructure Limited ISO 55000 Asset Management gap analysis assessment’. This has been deferred to 2024/25 after an initial external review in 2023, and

(b) Trams On-Track Plant and Machines. This has been deferred as the audit was intended to verify the actions from the 2022 audit have been effective. The audit actions have not yet been fully implemented.

6 Performance and Trends

6.1 There were 88 QSSA audits issued in the last four quarters (Quarter 3 of 2022/23 to Q2 2023/24), a decrease from 97 issued in the previous four quarters. The distribution of audits across Enterprise Risks and Chief Officers is generally consistent across the last two years. The breakdown of these audits in the last four quarters is as follows.

(a) 48 audits against ER1 (including the Integrated Systems audits in (b) below);

(b) 27 Integrated Systems audits (assessing LU operational and maintenance team compliance with a range of management system requirements including SHE, competence and finance);

(c) four audits against ER3 (in previous years ER3 audits were included in ER1);

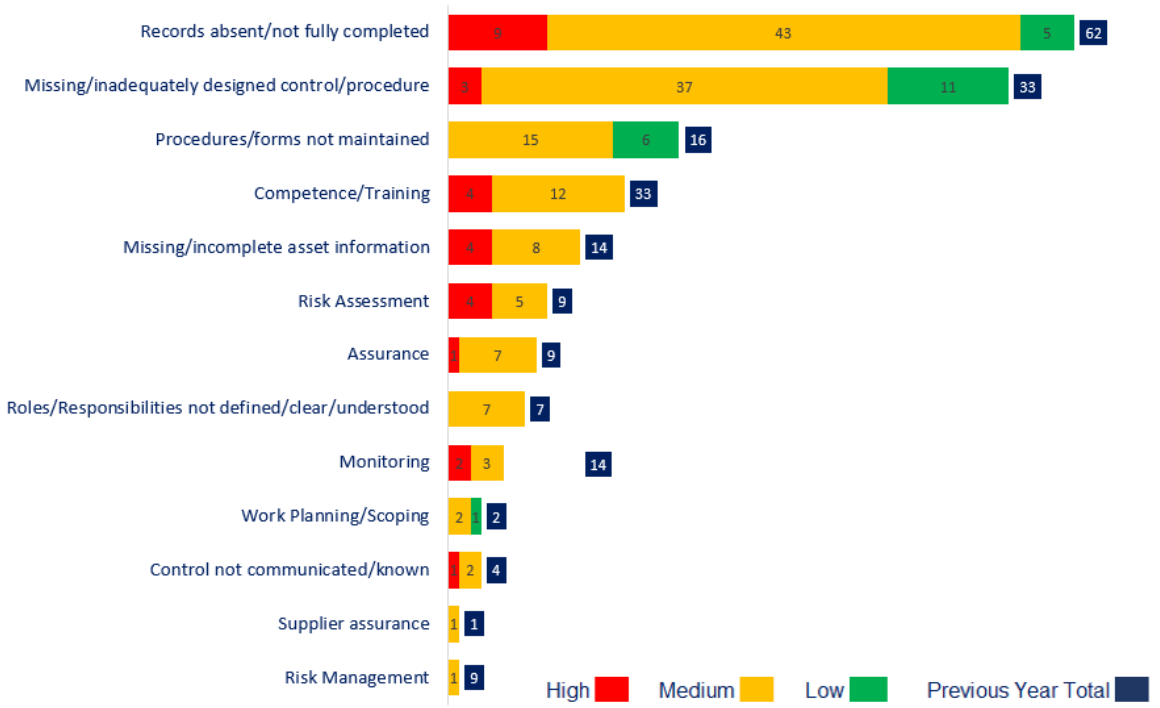
(d) 14 audits of TfL asset quality and compliance with internal or industry standards against ER6; and

(e) 22 audits against ER4 comprising of 20 Payment Card Industry Data Security Standard (PCI DSS) compliance audits and two audits against TfL standards or legislation.

6.2 The audits in the last four quarters were concluded as eight 'well controlled', 24 'adequately controlled', 19 'requires improvement' and four 'poorly controlled'. Comparing the last two years, there has been an increase in the number of 'requires improvement' conclusions in the last four quarters compared with the four quarters prior to that, increasing from 14 percent to 22 percent of the total (see Appendix 2). In the same period of time the percentage of 'adequately controlled' conclusions has reduced from 42 to 27 percent. The biggest difference is the increase in PCI DSS audits concluded as 'requires improvement' and reduction in audits concluded as 'adequately controlled'. Common themes from the PCI DSS audits are employee training, asset records and maintenance of roles and responsibilities during organisational change. Annual training is monitored via TfL's internal online 'Ezone' training site and reminders provided via email to ensure users remain up to date with requirements.

6.3 Individual audit findings with actions are codified to allow for greater trend analysis (see Graph 1 below). The most commonly occurring findings relate to non-compliances with TfL management systems, industry standards or legal requirements, this is consistent with the nature of our assurance work at the second line of defence. These non-compliances predominately manifest as 'missing/incomplete records' or 'ineffective procedures' which are both primary sources of evidence for an auditor. This theme was highlighted as a business issue in the 2022/23 TfL Annual Audit Opinion submitted to the Audit and Assurance Committee in June 2023. Competence and training records have fallen from the third to the fourth most common finding following a period of increased focus in 2022/23. Ensuring management systems documents are up to date and strengthening assurance at the first line would reduce the number of findings in these categories.

Graph 1: QSSA Audit Findings Q3 2022/23 – Q2 2023/24



6.4 Work continues on the management of actions, particularly overdue actions with management teams and the Chief Officers. There has been a significant improvement in the management of actions in 2023/24, with the lowest number of actions over 100 days for a number of years. However, there has been an overall increase in the number of overdue actions in Q2. The work to address the number of actions over 100 days overdue has been effective and we will work with the senior leadership to similarly address the other overdue actions.

6.5 At the end of Q2 there were 51 overdue actions out of 100, with 14 more than 100 days overdue. This compares with 26 overdue out of 113, with 11 over 100 days overdue at the end of Q1. The number of actions closed on time steadily increased in the past six months from 38 to 42 per cent (40 to 61 actions) and there has been a decrease in the number of actions extended from 19 to nine per cent (20 to one action).

7 SHE Directorate Assurance Update

7.1 In Q2, configuration of the pan-TfL digital assurance tool (iAuditor) was completed for Network Management and Resilience. This almost completes full rollout in TfL Operations. SHE is currently configuring iAuditor for the Asset Performance and Delivery business areas.

7.2 As part of our development of TfL's capability to provide SHE assurance systematically and consistently across our local management teams, local manager SHE checks have been developed. These digital assurance checks focus on SHE systems/ process compliance, enabling local managers to easily check how well they are complying with SHE Management System requirements. The checks will be made fully available to local managers in Quarter 3.

7.3 SHE has started an assurance and benchmarking activity, to identify how well local business areas are planning SHE assurance activities, carrying out SHE activities, checking the outcomes of assurance activities, and acting on the outcomes of SHE assurance activities. Our digital SHE assurance tool will be used to capture and analyse the data. The purpose of the activity is to benchmark how mature each business area is, in relation to SHE assurance, and will provide baselines for key SHE assurance activities such as local inspections (Planned General Inspections) and SHE Leadership Engagement Tours. It will also provide the opportunity to further promote the use of our digital SHE assurance tool within the business.

7.4 SHE assurance data from our digital SHE assurance tool is now being reported on the TfL Operations Thematic Scorecard. The Manager Inspections metric measures key SHE assurance activities across TfL Operations. The first activities to be reported are local inspections (Planned General Inspections) and SHE Leadership Engagement Tours. Initially, this will be a target-free metric for the whole of TfL Operations. The metric will then be developed to include a breakdown by business areas and completion against baselines established with the respective business areas by the end of the financial year.

7.5 SHE has started working with the Chief Capital Officer's area to develop a SHE assurance metric for Capital. This metric will include Planned General Inspections completed vs planned, SHE Leadership Engagement Tours completed vs planned and compliance with requirements in the SHE Management System. The plan is to start reporting as shadow metrics from Quarter 1 of 2024/251 2024/25. SHE will update the Panel further as development progresses.

List of appendices:

Appendix 1: QSSA Audits Completed in Q2 against ER1, ER3, ER4 and ER6

Appendix 2: QSSA Audit Data

List of Background Papers:

None

Contact: Mike Shirbon, Head of Quality, Safety and Security Assurance
Email: Mike.shirbon@tube.tfl.gov.uk

Appendix 1 – Quality, Safety and Security Assurance Audits Completed in Quarter 2 of 2023/24

ER1 Inability to deliver safety objectives and obligations

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Rail and Sponsored Services	23 705	London Overground (LO) Incident Investigation Process	To assess compliance and effectiveness of process, particularly following up on recommendations regarding investigations and cascade of learnings.	Adequately Controlled	The general management of incident reports and recommendations was evidenced to a consistent and satisfactory standard. Two observations were raised.
Asset Performance Delivery	23 704	London Underground (LU) Management of Lift and Escalator Incidents	To assess whether lift and escalator incidents are being reported, investigated and processed in accordance with procedure PR0775	Requires Improvement	LU Management of Lift and Escalator Incidents: elements of procedure PR0775 did not fully reflect current practices and requires updating to ensure there is a consistent understanding amongst stakeholders of key definitions and decision points following an incident.
Rail and Sponsored Services	23 706	Trams Incidents and Accidents Process Compliance	To assess compliance with the trams incidents and accidents procedure	Requires Improvement	There was good evidence of communication between TfL and Trams Operating Limited regarding significant incidents. Some requirements of the procedure were not sufficiently evidenced and are the focus of the agreed actions.
Engineering and Asset Strategy	23 726	LU Jubilee Northern Piccadilly lines Signal Engineers Competence Management	To check compliance with the Institution of Railway Signal Engineers (IRSE) requirements for signalling competence	Well Controlled	The requirements of the IRSE standard for competence of signalling staff were fully evidenced.

Integrated Systems Audits

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Asset Performance Delivery	23 741	Neasden Depot Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	79.4 per cent Conformance, 50 Green, 3 Amber, 10 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	23 728	Warwick Avenue Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	93 per cent Conformance, 51 Green, 1 Amber, 3 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	23 734	Amersham Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	68 per cent Conformance, 36 Green, 1 Amber, 16 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	23 735	Colliers Wood Area Stations Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	73 per cent Conformance, 38 Green, 1 Amber, 13 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	23 733	LU Mansion House Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	68 per cent Conformance, 39 Green, 18 Red (compliant, minor non-compliance, major non-compliance)
Customer Operations - LU	23 736	Knightsbridge Area Integrated Systems Audit	To provide assurance that key requirements contained in the management system are being met	Not Rated	66 per cent Conformance, 38 Green, 2 Amber, 18 Red (compliant, minor non-compliance, major non-compliance)

ER3 Environment including climate adaptation

Nil.

ER4 Significant security incident

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings

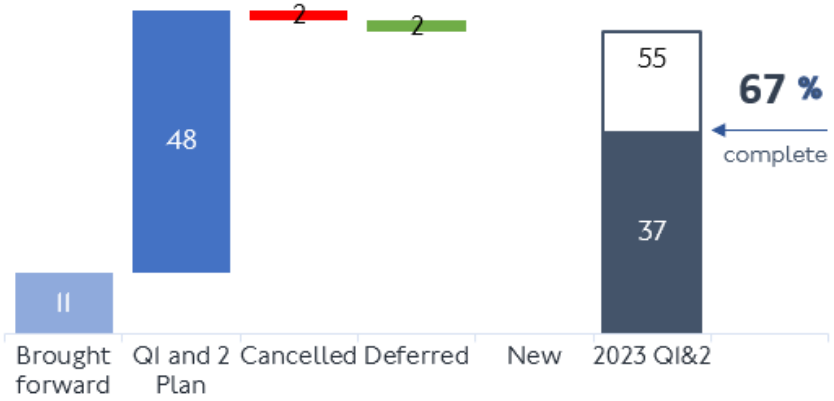
Chief Operating Officer	23 742	Payment Card Industry Data Security Standard (PCI DSS) Compliance Audit: Bus Stop Closures	To seek assurance that the Bus Stop Closures is operating in compliance with the PCI DSS v4.0 and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The Bus Stop Enforcement team was found to be operating in compliance with the PCI DSS.
Chief Customer and Strategy Officer	23 745	PCI DSS Compliance Audit: Art on the Underground (AoU)	To seek assurance that the AoU team is operating in compliance with PCI DSS v3.2.1 and additionally TfL's contractual obligations to it Acquiring Banks.	Adequately Controlled	The AoU team are not currently taking card payments or in the past 12 months and are not using the card machine which remains securely stored within the office.
Security, Policing and Enforcement	23 748	PCI DSS Compliance Audit: Compliance, Policing Operations and Security	To seek assurance that Compliance, Policing Operations and Security is operating in compliance with the PCI DSS v.4.0 and additionally TfL's contractual obligations to its Acquiring Banks.	Adequately Controlled	The external PCI Qualified Security Assessor recommended the exclusion of TfL Compliance, Policing Operations and Security from TfL's PCI DSS scope on the basis that PCI DSS does not supersede the requirement for TfL to support statutory legislation and byelaws in relation to the investigation and prosecution of crime.
Business Services	23 750	PCI DSS Compliance Audit: Staff Travel	To seek assurance that Staff Travel 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 Staff Travel team are not currently taking card payments and are not using the payment card machine which remains securely stored within the office.
London Transport Museum	23 743	PCI DSS Compliance Audit: TfL and London Transport Museum (LTM) Operations Centre	To seek assurance that the LTM Operations Centre are operating in compliance with the PCI DSS v4.0 and additionally TfL's contractual obligations to its Acquiring Banks.	Requires Improvement	The LTM Operations Centre was found to be non-compliant to the PCI DSS. Employee training was out of date and key manuals needed updating to reflect recent changes to the ticketing systems in use.
Chief Customer and Strategy Officer	23 744	PCI DSS Compliance Audit: TfL and LTM Shop	To seek assurance that the LTM shops are operating in compliance with the PCI DSS v.4.0 and additionally TfL's contractual obligations to its Acquiring Banks.	Requires Improvement	The LTM Shop was found to be non-compliant to the PCI DSS. The documentation regarding staff training and asset data was out of date and missing key information.

ER6 Deterioration of operational performance

Directorate	Ref.	Audit Title	Objective	Conclusion	Summary of Findings
Network Management and Resilience	23 707	Surface Asset Operations Electrical Inspections	To provide assurance that the recommendations from the previous audit have been fully implemented and are effective	Adequately Controlled	The significant changes implemented across the Asset Operations team and the controls from the previous audit 21 735 remain effective. The data migration plan to the Maximo system and detailed audit programme are in progress and monitored by the regular Continued Safe Operation meeting. Three medium and one low priority issues and two good practices were raised for this audit.
Rail and Sponsored Services	23 720	LO ISO 55000 Asset Management Assessment	To assess the LO Asset Management System using the Institute of Asset Management self-assessment methodology	Memo	The assessment identified that the LO Asset Management System maturity met most of the ISO 55000 standard. Areas that need to mature and will be included in LO improvements plans were competence, updating documented information, audit and corrective action and management review.
Asset Performance Delivery	23 723	LU Wimbledon Branch, Assurance of Network Rail Signal Maintenance	To test compliance with contractual requirements and standard S1532	Well Controlled	The was good evidence of compliance with the LU standards and contractual agreement.

Appendix 2 : Quality Safety Security Assurance Audit Summary Q2 2023/24

Audit Progress against Q1 and 2 2023/24 Plan

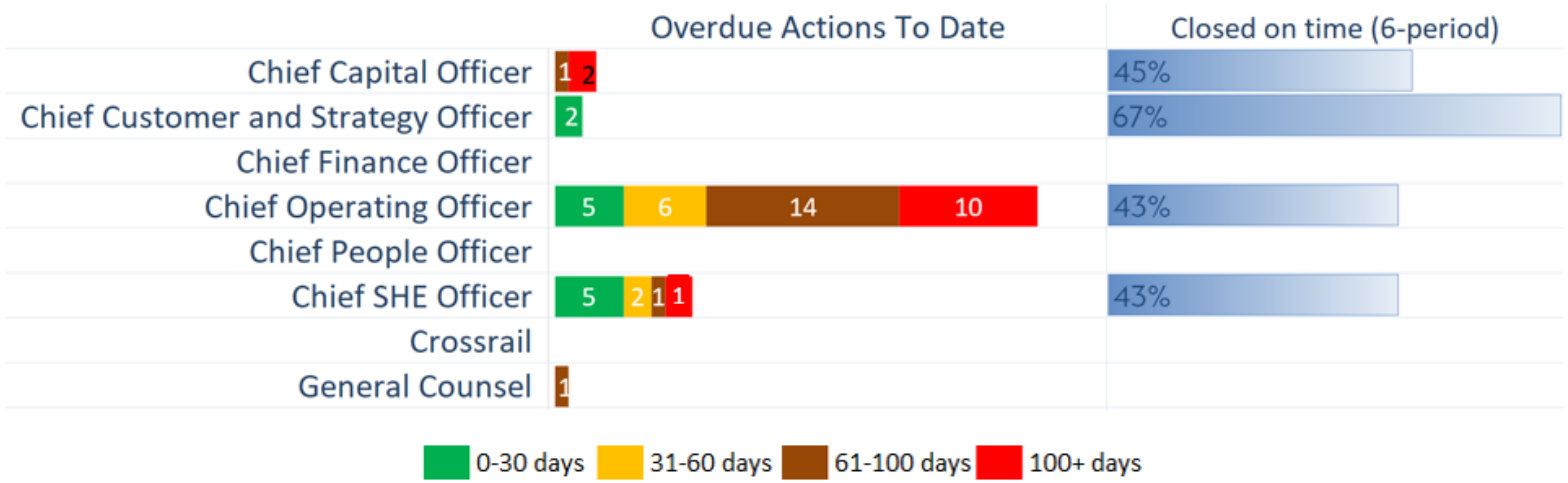


Open Audit Actions - Overall TfL Performance (6-Period trend)

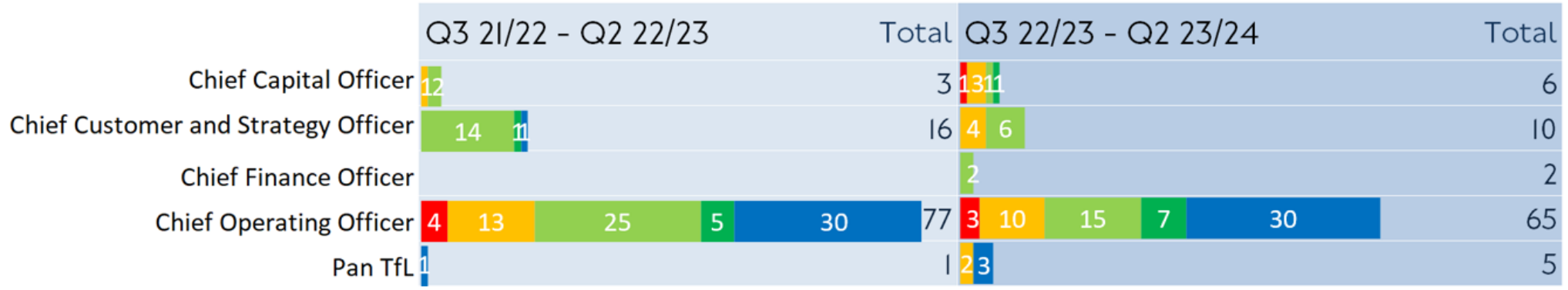
Measure	No.	%	6-period rolling trend
No. Actions Closed on time	61	42%	
No. Actions Extended	1	9%	

51 Overdue
Out Of
100 Open

Action Management - By Directorate by Overdue Days



Audit Conclusion Comparison by Chief Officer Team (over 4 quarters)



Audit Conclusion Comparison by Enterprise Risk (over 4 quarters)