Safety and Security Panel

Date: **12 February 2025**

Item: **Risk and Assurance Report Quarter 3 2024/25**

This paper will be considered in public

1 Summary

1.1 This report provides the Panel with an overview of the status of and changes to Enterprise Risk 01 (ER01) – 'Inability to deliver safety objectives and obligations', and Enterprise Risk 04 (ER04) – 'Significant security incident including cyber security'.

1.2 This report also summarises the findings from the associated assurance activity of these risks based on second line of defence audit work by the Quality, Safety and Security Assurance (QSSA) team and third line of assurance work by the Internal Audit team within TfL's Risk and Assurance Directorate. The paper covers the work during Quarter 3 of 2024/25 (15 September to 7 December 2024) (Q3).

1.3 A paper is included on Part 2 of the agenda which contains supplementary information that is exempt from publication by virtue of paragraphs 3 and 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to the financial and business affairs of TfL and information relating to any action taken or to be taken in connection with the prevention, investigation or prosecution of crime. Any discussion of that exempt information must take place after the press and public have been excluded from the meeting.

2 Recommendation

2.1 **The Panel is asked to note the paper and the exempt supplementary information on Part 2 of the agenda.**

3 TfL Enterprise Risks

3.1 Work is in progress to review and update ER01 including amending the title to reflect what this risk now covers and it will be presented at the TfL Executive Committee on 10 April 2025. An update will then be presented to this Panel on 19 May 2025. ER04 was updated following the cyber incident and discussed at the TfL Executive Committee on 5 December 2024 and is elsewhere on the agenda of this meeting.

4 Annual Audit Plans

4.1 The annual QSSA and Internal Audit plans contain a series of audits at the second line and third line respectively that address ER01 and ER04. Audits against other Enterprise Risks are also reported to the applicable Committee or Panel as well as the Audit and Assurance Committee.

4.2 The Internal Audit plan for the second half of 2024/25 was approved by the Audit and Assurance Committee on 18 September 2024 and will continue to be updated as appropriate to facilitate any additional audits that might be required because of the cyber incident. The QSSA audit plan has been shared with all risk owners and audit sponsors for consultation in line with our process. Internal Audit and QSSA both commenced audit planning for 2025/26 in Q3 in consultation with key stakeholders across TfL and owners of ER01 and ER04 risks and controls.

5 Work of Note this Quarter

5.1 Appendix 1 provides details of the Internal Audit and QSSA audits undertaken in Q3. 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.

Internal Audit

5.2 In Q3 Internal Audit issued two audits against ER01: 'Medical Assistance Programme Governance' and 'Use of Body Worn Video Cameras'. Additional information is provided in Appendix 1.

5.3 Three Internal Audits were in progress at the end of Q3 against ER04: 'Obsolescence of critical hosting software platforms'. Two audits were paused so as to not impact cyber incident recovery, 'Effectiveness of monitoring and patching of TfL's supply chain (Capita)' is due to restart in February 2025 and a new date for 'Effectiveness of Monitoring and Patching of TfL's Supply Chain (Cubic)' will be agreed with the business.

Quality, Safety and Security Assurance

5.4 Fourteen second line QSSA audits were delivered in Q3 against ER01 and there were no QSSA audits completed against ER04. Three were audits of TfL suppliers and concluded as 'well controlled' (two protection suppliers and Alstom Elizabeth Line fleet maintenance). Audits of 'London Underground (LU) Stations and Trains Competence Management System' and 'Elizabeth Line Safety Reporting' were both concluded as 'adequately controlled'. The audit of 'TfL Operations: Bus Station and Network Traffic Control - SHE (safety, health and environment) Compliance' was concluded as 'requires improvement'. Additional information is provided in Appendix 1.

5.5 Eight Integrated Systems Audits were competed in Q3. Integrated Systems Audits assess LU Operations teams' compliance with a range of risks and management system requirements and are therefore not rated. Additional information is provided in Appendix 1.

5.6 All the above audits have an agreed and tracked action plan in place.

5.7 No QSSA audits against ER04 were in progress at the end of Q3. Six QSSA audits against ER01 from the 2024/25 plan were in progress at the end of Q3:

(a) Managing SHE in our Supply Chain (sourcing);

(b) Docklands Light Railway Safety Authorisation Compliance;

(c) Trams Fleet Management of Fatigue;

(d) High Barnet Area Integrated Systems Audit;

(e) Greenwich Generating Station Integrated Systems Audit; and

(f) Turnham Green Area Integrated Systems Audit.

Counter-Fraud and Corruption

5.8 The Counter-Fraud and Corruption team investigate all allegations of fraud and corruption against TfL involving TfL employees, non-permanent labour and third parties (including suppliers, customers and organised criminals). These cases are part of the wider fraud reporting that is submitted to the Audit and Assurance Committee.

6 Cancelled and Deferred Work

6.1 One Internal Audit against ER04 was cancelled in Q3, 'Cubic Risk Management', so as to not impact on cyber incident recovery work and will be rescheduled. Details of two deferred audits are provided in paragraph 5.3 above.

6.2 Fifteen audits against the Payment Card Industry Data Security Standard (PCI DSS) that relate to ER04 have been cancelled in Q3 as these audits will now be undertaken by TfL Technology and Data Payment Operations and Assurance team. One audit of 'Management of Fatigue Risk: Bus Operating Contractors' was cancelled for 2024/25 in Q3 as it was identified in planning that work was underway to develop, test and pilot in vehicle fatigue detection technology.

7 Performance and Trends

7.1 Performance data is provided in Appendix 2 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.

Internal Audit

7.2 Eleven ER01 and ER04 internal audits were completed in the last four quarters compared with four in the preceding four quarters. This is due to an increase in the number of ER04 audits identified through our risk-based approach to internal audit planning.

7.3 At the end of Q3 there were 24 open Internal Audit actions against ER01 and ER04, 10 of which were overdue, three by less than 30 days, three by 30-60 days and four by 61-100 days. Over the last six periods there has been a steady increase in the number of actions closed on time and a reduction in the number of actions extended.

Quality, Safety and Security Assurance

7.4 Comparing the number of ER01 and ER04 QSSA audits for Quarter 4 (Q4) of 2022/23 to Q3 2023/24 (66 audits) with Q4 2023/24 to Q3 2024/25 (53 audits) there has been a reduction in the number of audits completed by 20 per cent as this year's audit delivery has been impacted by staff turnover. The distribution of conclusion by Chief Officer team is broadly consistent, with the majority of audits being conducted in the Chief Operating Officer's team, with a small reduction in the number of audits for the Chief Capital Officer, Chief Finance Officer and Chief People Officer teams. Comparing conclusion by Enterprise Risk there is a notable reduction in audits against ER04 from 21 to 10, this is mostly due to the change in responsibility for PCI DSS audits (see paragraph 6.2 above).

7.5 The distribution of audit conclusions is consistent across the two years (within five per cent) except for the reduction in audits concluded as 'requires improvement'. There were eight fewer 'requires improvement' audits against ER04 in the last four quarters, previous 'requires improvement' audits were all PCI DSS audits.

7.6 Work continues on the close out of management of QSSA actions, particularly overdue actions with management teams and the relevant Chief Officer. At the end of Q3 there were 17 overdue actions for ER01 and ER04 out of 42 open actions with six overdue by 100 days or more (five of which have been closed since the end of Q3), four overdue by less than 30 days and seven overdue by 30-60 days. All actions that are overdue by more than 100 days are reported to the Audit and Assurance Committee and are discussed with Chief Officers.

List of appendices:

Appendix 1: QSSA and Internal Audits Completed in Q3 against ER01 and ER04

Appendix 2: QSSA and Internal Audit Summary

A paper containing exempt supplementary information is included on Part 2 of the agenda

List of Background Papers:

None

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

Appendix 1 – Quality, Safety and Security Assurance Audits Completed in Quarter 3 of 2024/25

ER01 Inability to deliver safety objectives and obligations

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 762	Supplier Audit: Alstom Elizabeth Line	Seek assurance that Alstom is assuring its health and safety accountabilities under the contract for Elizabeth line rolling stock maintenance.	Well Controlled	Alstom assurance of its occupational safety accountabilities for rolling stock maintenance are managed using structured and planned assurance activities. These activities include Planned General Inspection, High Hazard Inspections, Control of Contractor's Performance Review, Safety Observation Visits, Surveillance Audits and Internal Audits. Actions resulting from assurance activities are managed using PowerBI and relevant databases.
Chief Operating Officer	24 763	Elizabeth Line Safety Reporting	Seek assurance that effective safety reporting systems are in place to report at regular intervals performance to leaders so they can review and be assured that legal compliance is achieved and maintained, and continuous improvement generated.	Adequately Controlled	There are structured systems and procedures for effective safety reporting within RfLI to ensure legal compliance. Reporting roles and responsibilities relating to proactive and reactive monitoring of safety performance are well defined. Safety data is collated using databases and Safety Culture Application; analysed using PowerBI and reported to senior management via periodic reporting packs.
Chief Operating Officer	24 715	TfL Operations Bus Station and Network Traffic Control – Safety, Health, Environment (SHE) Compliance	Seek assurance that TfL Operations Bus Station and Network Traffic Control are suitably managing their (SHE) risks through compliance with TfL SHE Management System.	Requires Improvement	There were controls in place for most risks however, management assurance was limited as there were no formal programme or completion of Planned General Inspections or Local Manager SHE Checks. Dissemination of SHE information between senior management and operational staff also needs improvement.
Chief Operating Officer	24 758 U	Protection Supplier Audit - 1st Inrail	Provide assurance that 1st Inrail are providing competent protection staff in accordance with contractual, Quality, Environmental, Safety and Health (QUENSH) and London Underground (LU) Standards requirements.	Well Controlled	1st Inrail Limited were found to be managing and providing competent protection staff and support activities in accordance with the contract QUENSH conditions and LU standards
Chief Operating Officer	24 759 U	Protection Supplier Audit - Global Media	Provide assurance that Global Outdoor Media are providing competent protection staff in accordance with contractual, QUENSH and LU Standards requirements.	Well Controlled	Global Outdoor Media Limited had established policies, procedures, and processes in place for managing and providing competent protection staff as stipulated in QUENSH requirement and associated LU standards.

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 734	LU Stations and Trains Competence Management System	Assess effectiveness and compliance of the Competence Management System for safety critical station and traincrew staff with Office of Rail and Road (ORR) Safety Publication 1 – Developing and Maintaining Staff Competence.	Adequately Controlled	The system design and implementation were generally compliant with ORR expectations. Areas for strengthening were using a broader range of Key Performance Indicators to monitor and report on compliance with the system and specifically attendance of classroom-based training in stations.

Integrated Systems Audits

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 714	Emergency Response Unit Integrated System Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	70 per cent conformance
Chief Operating Officer	24 707	Mornington Crescent Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	53 per cent conformance
Chief Operating Officer	24 708	Whitechapel Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	52 per cent conformance
Chief Operating Officer	24 709	Arsenal Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	62 per cent conformance
Chief Operating Officer	24 711	Jubilee North Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	59 per cent conformance
Chief Operating Officer	24 783	Charing Cross Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	75 per cent conformance
Chief Operating Officer	24 786	Seven Sisters Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	59 per cent conformance
Chief Operating Officer	24 791	Earls Court Traincrew Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met	Not Rated	47 per cent conformance

Internal Audit: Draft reports issued in Quarter 3 of 2024/25

ER01 Inability to deliver safety objectives and obligations

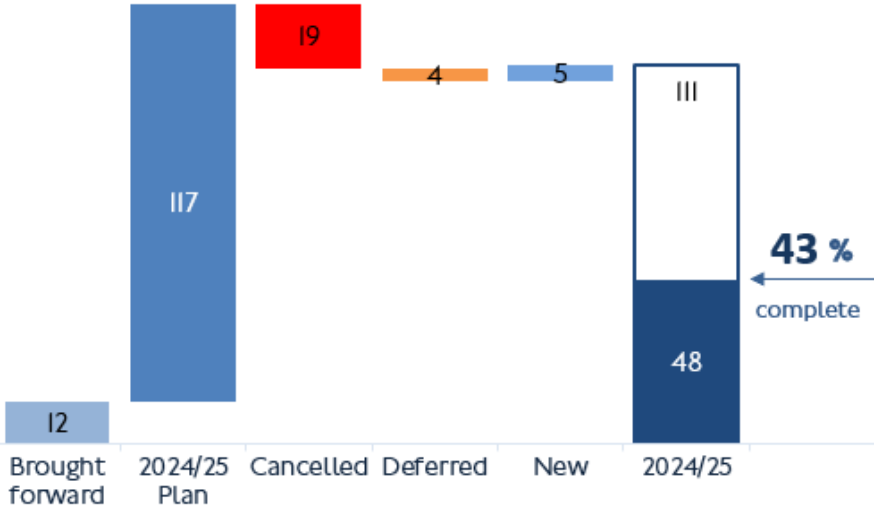
Chief Officer	Ref	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Safety Health and Environment Officer	24 001	Medical Assistance Programme (MAP) Governance	Provide assurance on the adequacy and effectiveness of key controls for managing the MAP.	Requires Improvement	There is a small, dedicated team that oversees the delivery and management of the MAP process. The Occupational Health Administrator oversees the administration of the end-to-end process. We found gaps in the documentation and process that do not reflect actual practice and if not addressed it would affect resilience in the team.
Chief Operating Officer	24 037	Use of Body Worn Video Cameras	Provide assurance on the adequacy and effectiveness of key controls for managing the implementation of body worn cameras.	Adequately Controlled	Implementation of Body Worn Video Camera (BWVC) has been successfully rolled out by the Workplace Violence and Aggression team. Although BWVC adoption by staff is generally good, site visits noted areas of patchy use, reducing the overall rate of compliance across the business to around 71 per cent. Three medium severity issues were noted around an out of date Data Protection Impact Assessment, improvements to the user dashboard to increase compliance and mandatory training of staff.

ER4 Significant security incident including cyber security

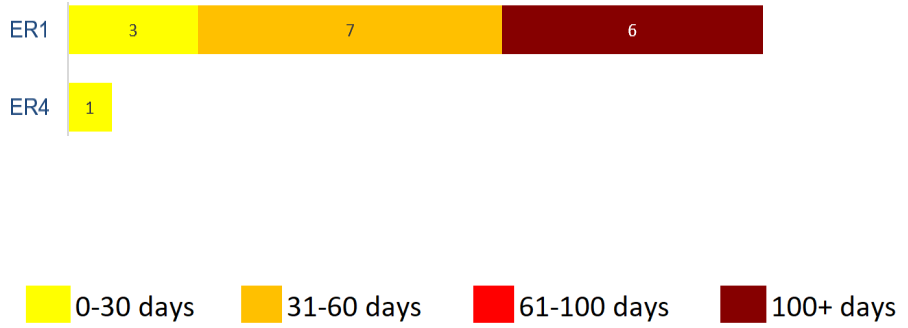
Chief Officer	Ref	Audit Title	Objectives	Conclusion	Summary of Findings
None					

Appendix 2 : Quality Safety Security Assurance Audit Summary

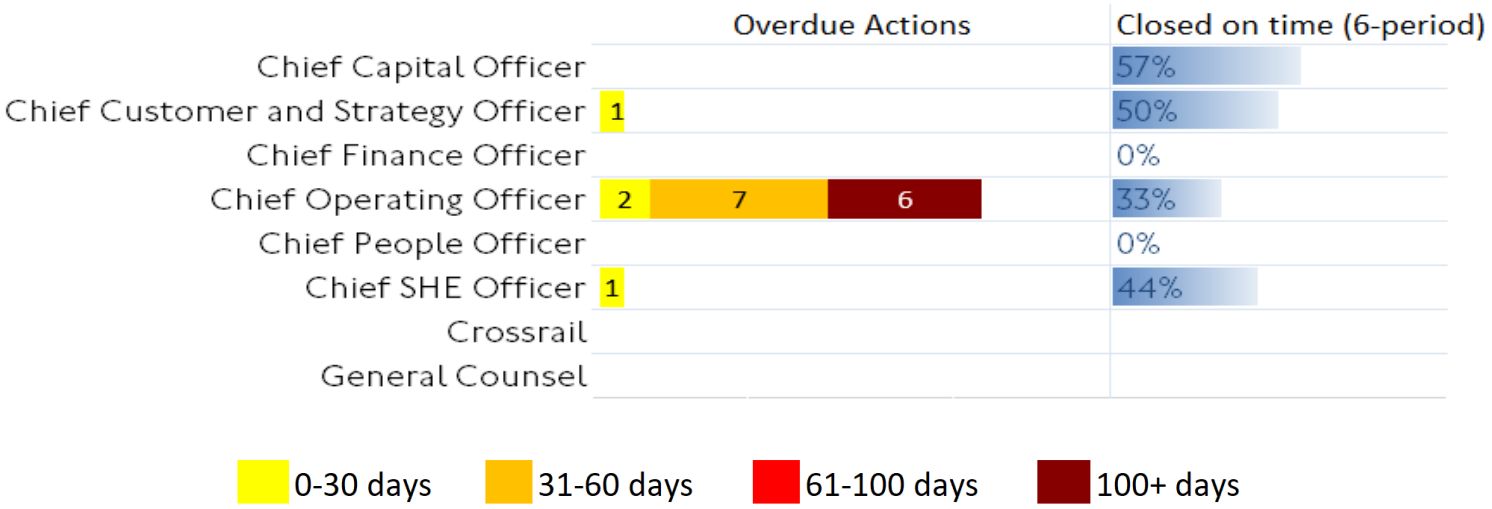
Audit Progress against 2024/25 Plan



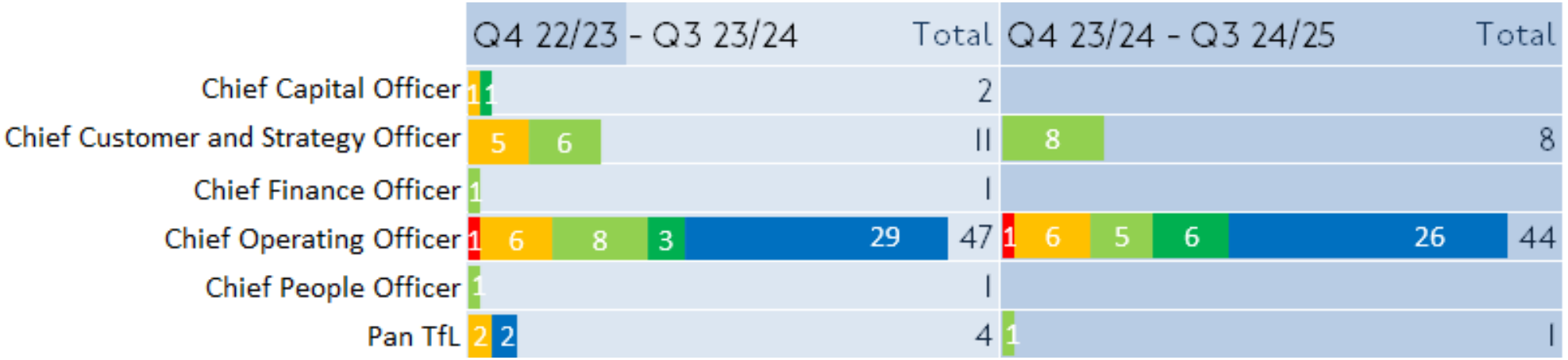
Action Management (ER01 and ER04) By Enterprise Risk by Overdue Days



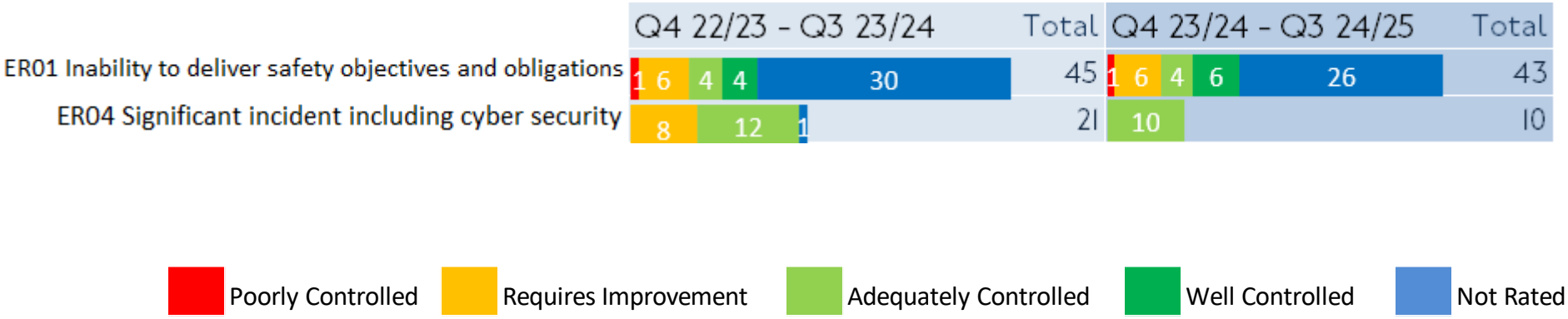
Action Management (ER01 and ER04) - By Directorate by Overdue Days



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

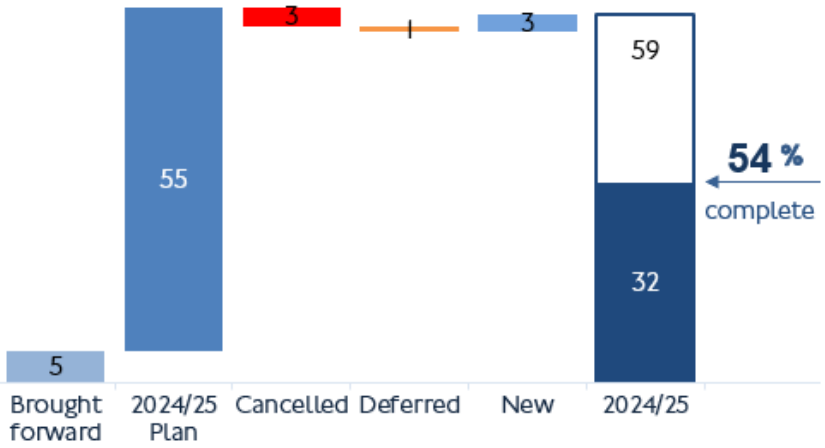


Audit Conclusion Comparison by Enterprise Risks (over 4 quarters)

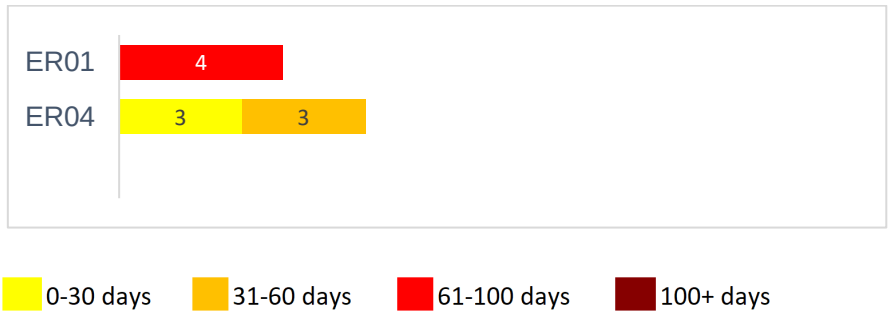


Internal Audit Summary Q3 2024/25

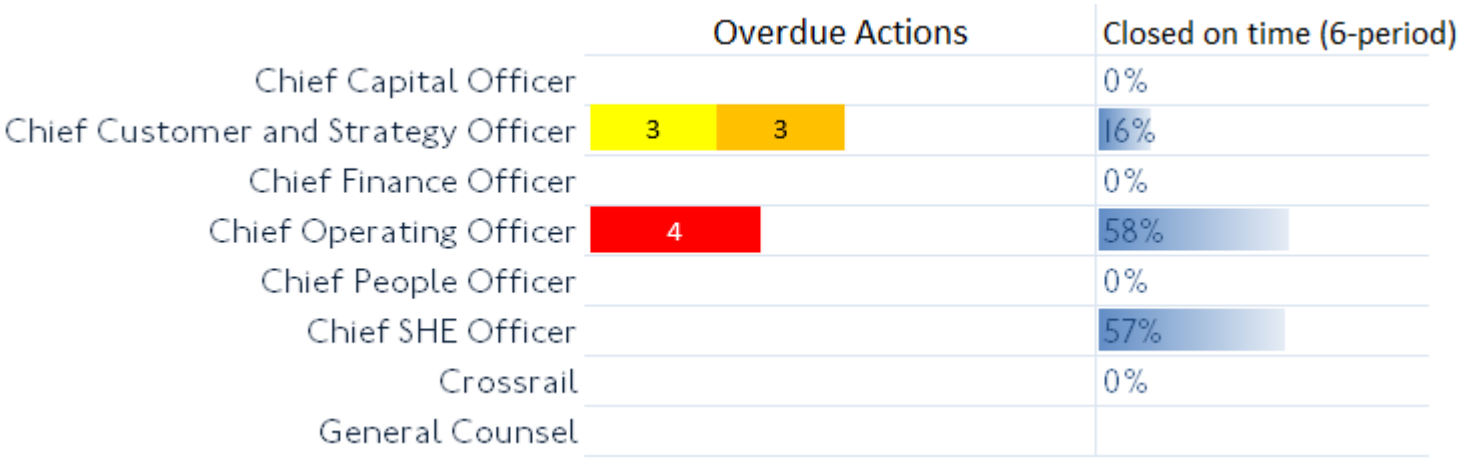
All Audit Progress against 2024/25 Plan



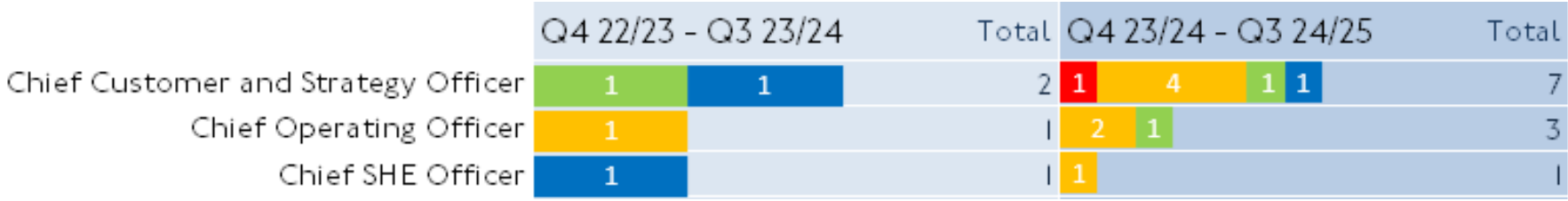
Action Management (ER01 and ER04) By Enterprise Risk by Overdue Days



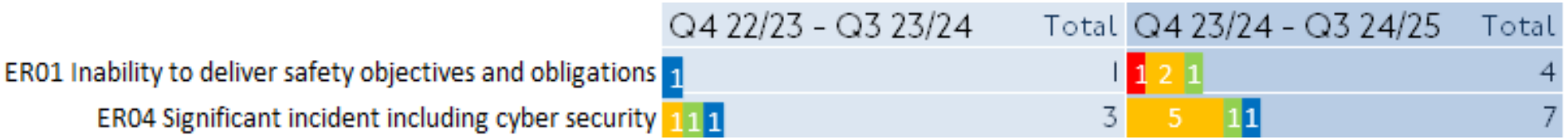
Action Management (ER01 and ER04) - By Directorate by Overdue Days



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



Audit Conclusion Comparison by Enterprise Risk (over 4 quarters)



Poorly Controlled | Requires Improvement | Adequately Controlled | Well Controlled | Not Rated