Safety and Security Panel

Date: **19 May 2025**

Item: **Risk and Assurance Report Quarter 4 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) – 'Failure to prevent a significant safety incident or deliver safety obligations', and Enterprise Risk 04 (ER04) – 'Significant security incident including Cyber Security'. ER04 will be split into two level 0 risks: ER04 – 'Significant security incident' and Enterprise Risk 11 – 'Significant cyber security incident' (ER11). This panel will receive separate updates on assurance work related to ER11 from April 2025.

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 4 of 2024/25 (8 December 2024 to 31 March 2025) (Q4).

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 or business affairs of TfL and 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 ER01 has been reviewed, updated and presented to the Executive Committee on 10 April 2025. ER01 risk title has changed from 'Inability to deliver safety objectives and obligations' to 'Failure to prevent a significant safety incident or deliver safety obligations'. A full update on ER01 is included elsewhere on the agenda for this meeting.

3.2 Following the cyber incident and previous discussions at the meeting of this Panel on 12 February 2025, a decision has been made to split out the cyber aspects of the risk from ER04 – 'Significant security incident including cyber security'. A new risk, ER11 – 'Significant cyber security incident' is in

development to cover Information Technology and Operational Technology. This will allow for greater focus on mitigations to bring about improvements. ER11 will be reviewed by the Executive Committee in May and then to the 2 September 2025 meeting of this Panel. A workshop has been scheduled to review and update the remaining aspects of ER04 which will come to the 12 November 2025 meeting of this Panel.

3.3 We will begin reporting assurance work against the updated risks including ER11 from Quarter 1 of 2025/26.

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 for 2024/25, as of quarter 1 2025/26 this will also include ER11. 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 first half of 2025/26 was approved by the Audit and Assurance Committee on 10 March 2025. The QSSA audit plan has been shared with all risk owners and audit sponsors for consultation in line with our process.

5 Work of Note this Quarter

5.1 Appendix 1 provides details of the Internal Audit and QSSA audits undertaken in Q4. 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. Where audits are shown as completed against ER04 in 2024/25, this refers to the former ER04: ‘Significant security incident including Cyber Security’.

Internal Audit

5.2 No Internal Audit work was completed against ER01 in Q4. Two Internal Audits were issued against the former ER04: ‘Artificial intelligence (AI) (implementation of Microsoft tools with built-in AI)’; and ‘London Transport Museum Business Continuity’. Additional information on these is provided in Appendix 1.

5.3 Two Internal Audits were in progress at the end of Q4 against the former ER04: ‘Effectiveness of Monitoring and Patching of TfL’s Supply Chain (Capita)’; and ‘Payments Technology Refresh’.

Quality, Safety and Security Assurance

5.4 Thirteen second line QSSA audits were delivered in Q4 against ER01 and there were three QSSA audits completed against the former ER04. The three ER04 audits were Payment Card Industry Data Security Standard (PCI DSS) compliance audits. Audits of 'Woolwich Ferry Safety, Health and Environment (SHE) Compliance' and 'London Underground (LU) Signalling Competence' were concluded as 'adequately controlled' and 'well controlled' respectively. The audit of 'DLR Safety Authorisation (Section 15: Asset Maintenance) Compliance' was concluded as 'requires improvement'. Additional information is provided in Appendix 1.

5.5 Ten integrated systems audits were competed in Q4. Integrated Systems Audits assess LU Operations and Asset Performance teams' compliance with a range of risks and management system requirements and are therefore not rated. Additional details are contained in Appendix 1.

5.6 All of 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 Q4. Six QSSA audits against ER01 from the 2024/25 plan were in progress at the end of Q4:

(a) Rail for London Infrastructure (RfLI) Managing Electricity at Work;

(b) RfLI Plumstead Depot SHE Compliance;

(c) Competence of Keolis Amey Docklands Maintenance Staff;

(d) Managing SHE in our Supply Chain – Sourcing stage;

(e) Places for London Constructions (Design and Management) Regulations (CDM) Client Duties; and

(f) Trams Managing Electricity at Work.

Counter-fraud and Corruption

5.8 The Counter-fraud and Corruption team investigate all allegations of fraud and corruption against TfL involving TfL employees (including 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 Four QSSA audits against ER01 have been deferred to 2025/26 due to staff turnover and one cancelled. These audits were 'Elizabeth Line Service Control Centre SHE Compliance', 'Managing safety related customer complaints' (deferred to align with other assurance activity), 'LU Managing Electricity at Work', 'LU Management of Manual Handling Risk' and an LU Integrated Systems Audit.

6.2 Four PCI DSS audits (ER04 related) were cancelled due to either the TfL team no longer taking payments or assurance being provided by the Payments team in Technology and Data.

6.3 Seven audits against the former ER04 were deferred to the 2025/26 plan due to staff turnover: 'Strategic Communications Plan', 'Management of TfL Supplier Cyber Security Risk', 'Light Rail Security Programme audits of DLR, Trams and LU' (three audits), 'Identification and Management of Security Risk in TfL Projects' and 'Management of Actions from Local Security Action Plans'. All have been discussed with the audit sponsor and owners of the controls to be audited.

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 Ten ER01 and (former) ER04 internal audits were completed in the last four quarters compared with five 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. A review of findings has highlighted a few instances where governance arrangements need tightening. These include an absence of clearly documented processes, as well as a lack of clarity on roles and responsibilities. We will continue to monitor this going forward.

7.3 At the end of Q4 there were 74 open Internal Audit actions against ER01 and former ER04, none of which were overdue. Over the last six periods there has been a slight decrease in the number of actions closed on time, however the number of actions extended remains consistent.

Quality, Safety and Security Assurance

7.4 The QSSA team managed to meet the target of 85 per cent of the plan being delivered by year end, this followed the plan being re-baselined mid-year to ensure it was consistent with team resources after staff turnover.

7.5 Comparing the number of ER01 and former ER04 QSSA audits for 2023/24 (86 audits) with 2024/25 (76 audits) there has been a reduction in the number of ER04 audits completed by 16 as it has been agreed that they will be undertaken by the Payments team in Technology and Data. The number of ER01 audits has remained relatively consistent and there has been an increase in audits undertaken against other Enterprise Risks, reported to other Committees and Panels.

7.6 The greatest difference in distribution of audit conclusion by Chief Officer team across the last two years is the reduction in 'poorly controlled' conclusions from two to none. The proportion of 'requires improvement' conclusions has remained the same but there is a noteworthy movement from 'adequately controlled' to 'well controlled' noted between the two years. The audit plan differs each year so direct comparisons are limited, however, the progress between the two years is encouraging.

7.7 A review of data from the Integrated Systems Audits has highlighted the most commonly occurring findings: risk assessment, competence management, fire safety compliance checks, emergency planning, and the effectiveness of local safety assurance checks. These have been discussed with the Operations team to be included in improvement work and is being discussed at the Executive Committee.

7.8 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 Q4 there were seven overdue actions for ER01 and ER04 out of 103 open actions with four overdue by 100 days or more (all four of which are from the same audit) and three that are between 30-60 days overdue. This compares with 14 actions of 100 days or more for the same time last year. 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 to this report:

Appendix 1: QSSA and Internal Audits Completed in Q4 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

[page left intentionally blank]

Appendix 1 – Quality, Safety and Security Assurance Audits Completed in Quarter 4 of 2024/25

ER01 Failure to prevent a significant safety incident or deliver safety obligations

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 772	Docklands Light Railway (DLR) Safety Authorisation (Section 15) Compliance	Assess DLR compliance with Section 15 of the Safety Authorisation - Maintenance of Assets.	Requires Improvement	Several referenced documents in the Safety Authorisation were not available at the time of the audit. Audits and other asset assurance activities described were not consistently planned and undertaken.
Chief Operating Officer	24 808	Woolwich Ferry Safety, Health and Environment (SHE) Compliance	Seek assurance that Woolwich Ferry are suitably managing their SHE risks through compliance with the TfL SHE Management System.	Adequately Controlled	Woolwich Ferry were able to demonstrate SHE risks were being suitably managed in compliance with the SHE Management System. There were a few areas where improvements could be made as identified in the actions.
Chief Operating Officer	24 823 U	London Underground (LU) Signalling Competence Institution of Railway Signal Engineers (IRSE)	Seek assurance that the procedure and associated activities covering Institution of Railway Signal Engineers (IRSE) Licensing within LU Assessing Agency meet the requirements of the awarding body.	Well Controlled	The processes and procedures in place fully meet the requirements of the relevant IRSE Licencing Standard and Procedures.

Integrated Systems Audits

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 784	Turnham Green Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	82 per cent conformance rate, 8 Major, 1 minor, 41 compliant
Chief Operating Officer	24 785	High Barnet Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	76 per cent conformance rate, 11 major, 1 minor, 39 compliant
Chief Operating Officer	24 787	Stepney Green Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	78 per cent conformance rate, 12 major, 0 minor, 43 compliant
Chief Operating Officer	24 788	Canada Water Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	72 per cent conformance Rate, 14 major, 1 minor, 38 compliant
Chief Operating Officer	24 789	West Ham Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	51 per cent conformance rate; 25 major, 1 minor, 27 compliant
Chief Operating Officer	24 790	Manor House Area Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	80 per cent conformance rate, 9 major, 2 minor, 43 compliant
Chief Operating Officer	24 792	Seven Sisters Traincrew Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	70 per cent conformance rate, 8 major, 2 minor, 23 compliant
Chief Operating Officer	24 793	Hammersmith Traincrew Integrated Systems Audits	Provide assurance that key requirements contained in the management system are being met.	Not Rated	72 per cent conformance rate, 10 major, 2 minor, 26 compliant

Chief Officer	Ref.	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 794	Harrow-On-The-Hill Traincrew Integrated Systems Audit	Provide assurance that key requirements contained in the management system are being met.	Not Rated	28 per cent conformance rate 28 major, 0 minor, 8 compliant
Chief Operating Officer	24 821 U	Greenwich Generating Station Integrated Systems	Provide assurance that key requirements contained in the management system are being met.	Not Rated	83 per cent conformance rate, 4 major, 5 minor, 47 compliant

ER04 Significant security incident

Chief Officer	Ref	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Operating Officer	24 746	Payment Card Industry Data Security Standard (PCI DSS) Compliance Audit: Taxi Private Hire Operator, Driver and Vehicle Licensing	Seek assurance that controls and systems are in place that meet the requirements of the PCI DSS.	Not Rated	The Taxi Private Hire Operator, Driver and Vehicle Licensing submitted their required self-assessment of compliance with the PCI DSS.
Chief Operating Officer	24 778	PCI DSS Compliance Audit: Victoria Coach Station (VCS)	Seek assurance that the VCS is operating in compliance with the requirements of the PCI DSS.	Not Rated	The VCS submitted their required self-assessment of compliance with the PCI DSS.
Chief Customer and Strategy Officer	24 817	PCI DSS Compliance Audit: Lost Property Office (LPO)	Seek assurance that controls and systems are in place that meet the requirements of the PCI DSS.	Not Rated	The LPO submitted their required self-assessment of compliance with the PCI DSS.

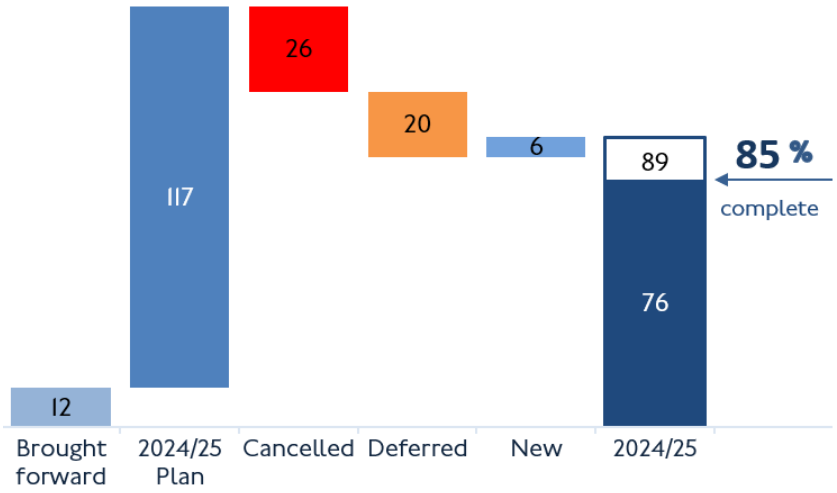
Internal Audit: Draft reports issued in Quarter 4 of 2024/25

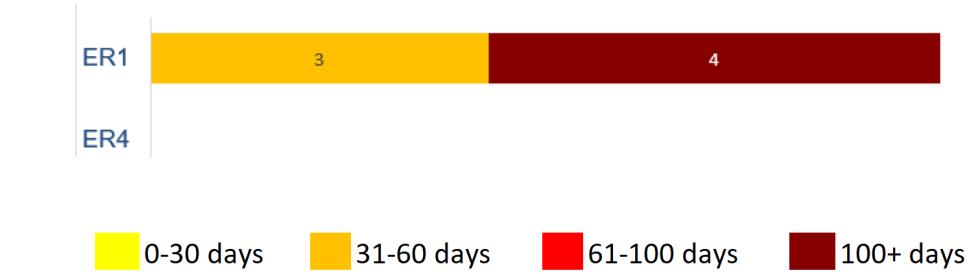
ER04 Significant security incident including cyber security

Chief Officer	Ref	Audit Title	Objectives	Conclusion	Summary of Findings
Chief Customer and Strategy Officer	24 049	Artificial Intelligence (AI) (implementation of Microsoft tools with built-in AI)	Assess and evaluate the adequacy and effectiveness of a selection of key controls in relation to the implementation of corporate tools with AI.	Requires Improvement	The audit found a lack of some technical controls to enforce the requirements of the TfL Generative AI policy
Chief Customer and Strategy Officer	24 051	London Transport Museum (LTM) Business Continuity	Provide assurance on the adequacy of LTM's business continuity process.	Requires Improvement	A comprehensive bottom-up Business Impact Analysis and corresponding business continuity risk identification and assessment exercise has not been done. Additionally, existing incident management plans do not consider all key risks and incident scenarios faced.

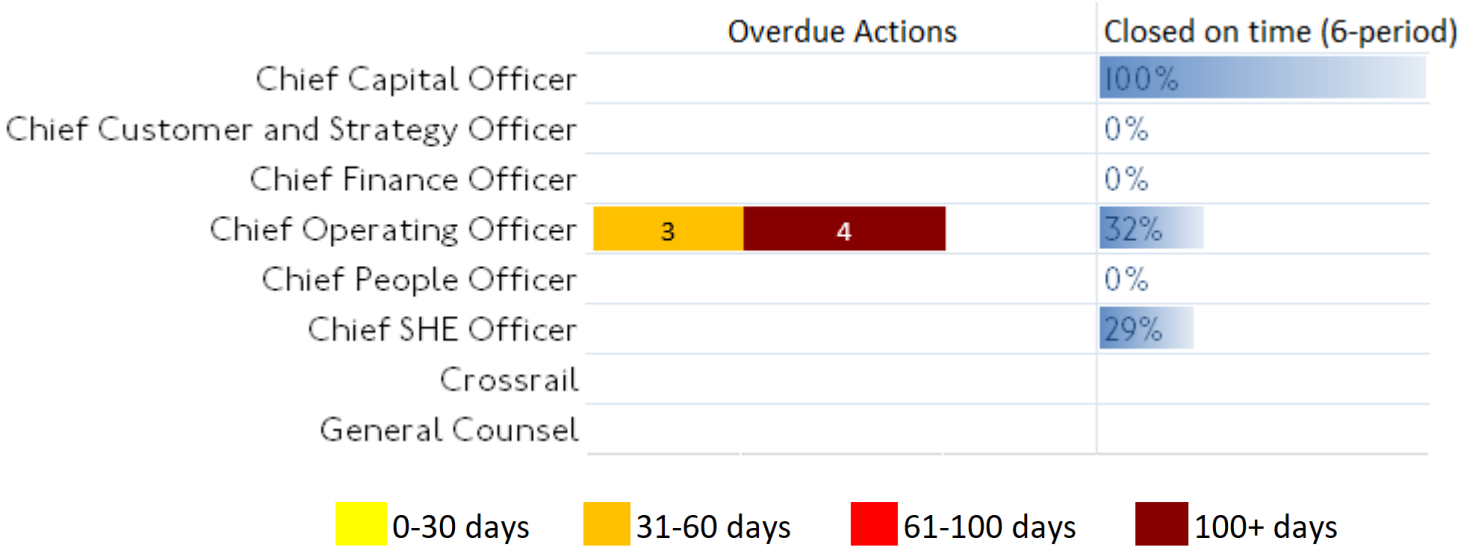
Appendix 2 : Quality Safety Security Assurance Audit Summary

Audit Progress against 2024/25 Plan

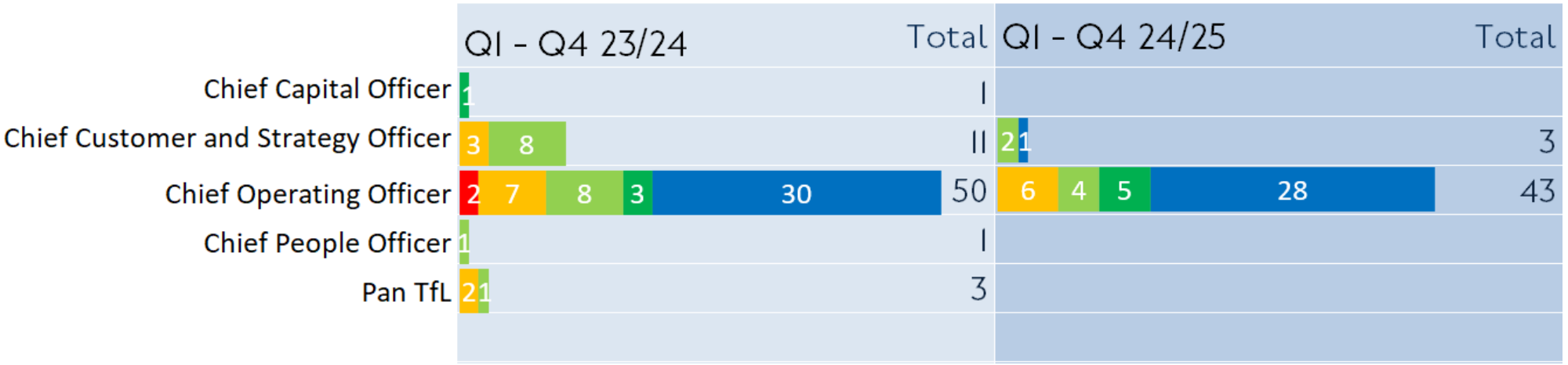




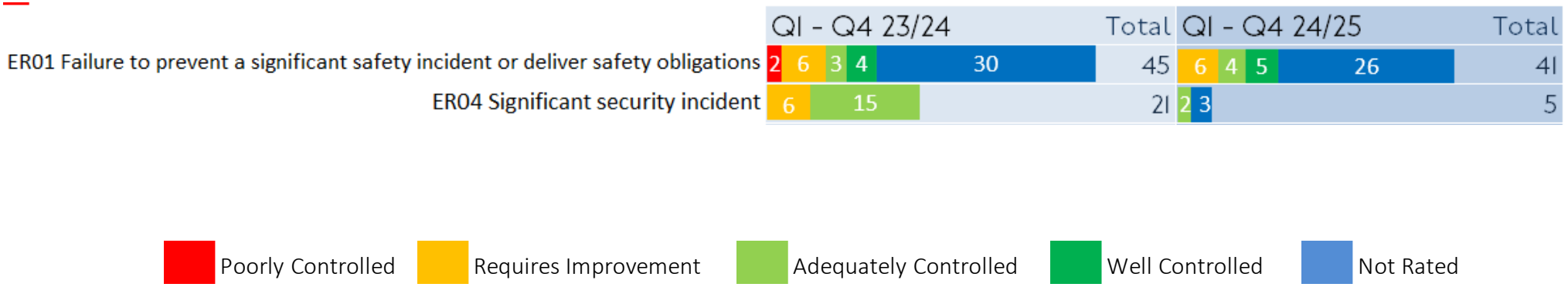
Action Management (ER01 and ER04) - By Directorate by Overdue Days



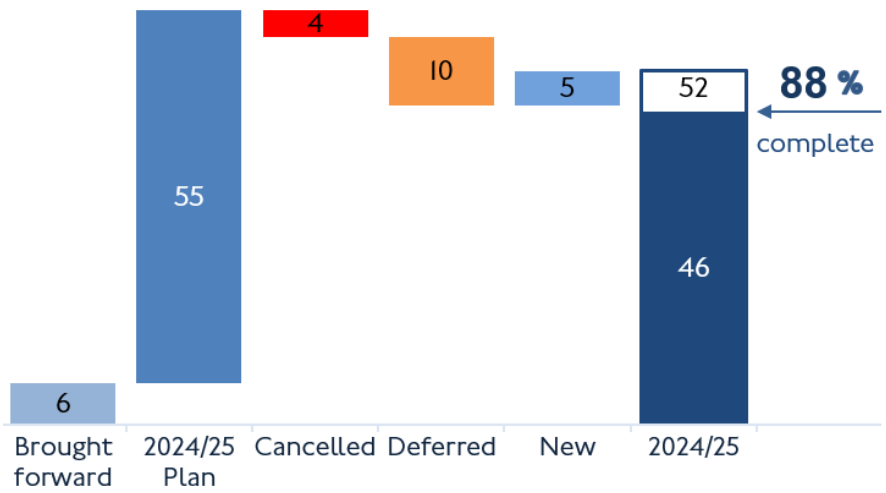
Audit Conclusion Comparison by Chief Officer Team (over 4 quarters) – ER01 and ER04



Audit Conclusion Comparison by Enterprise Risks (over 4 quarters)

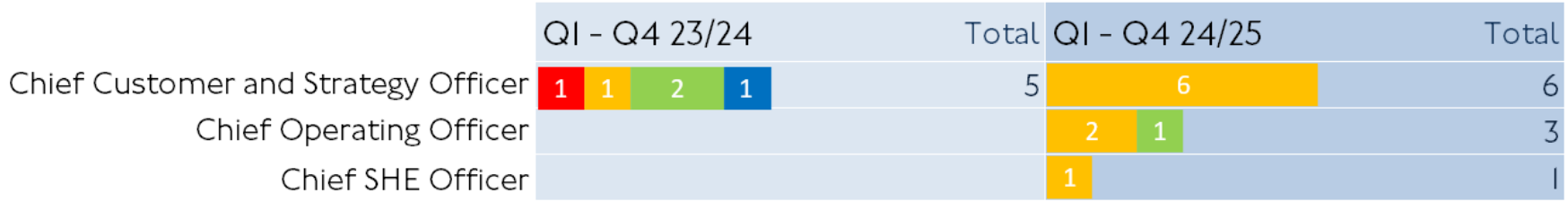


Internal Audit Summary

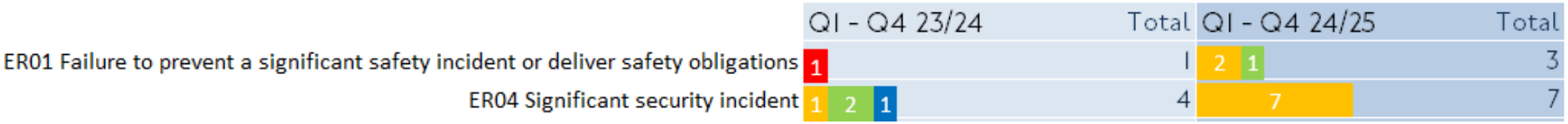


None

Audit Conclusion Comparison by Chief Officer Team (over 4 quarters) - ER1and ER04



Audit Conclusion Comparison by Enterprise Risk (over 4 quarters)



[page left intentionally blank]