Social Security Scotland
Tèarainteachd Shòisealta Alba

Audit and Assurance Committee

Quarter 2- June to August 2024

Dignity, fairness, respect.

Overall Social Security Scotland Risk Profile

Risk Description	Inherent	Residual	Score Change	Target Score	Gap to target	Control Confidence	Date to target score
CR-001 Workforce Planning	20	12	↔	8	4	Limited	Mar-25
CR-002 Fraud	25	20	↔	15	5	Limited	Apr-29
CR-003a Value For Money	20	12	↔	8	4	Limited	Mar-25
CR-003b Financial Management	25	20	↔	15	5	Substantial	Apr-25
CR-004 Quality	25	20	↔	15	5	Limited	Mar-25
CR-005 Performance, Culture and Inclusion	9	12	↔	6	6	Limited	Dec-24
CR-006 Technology and Systems	16	12	↔	9	3	TBC	Dec-24
CR-007 Safeguarding	20	16	↔	12	4	Limited	Aug-25
CR-008 Business Resilience	25	20	↔	15	5	Reasonable	May-26
CR-009 Delivering For Clients	25	20	↔	10	10	Limited	Dec-25
CR-010 Cyber Security	25	20	↔	10	10	Limited	TBC
CR-011 Programme Closure	25	25	↔	15	10	Insufficient	Apr-25
CR-012 Management Information and Performance (Data)	20	20	↔	16	4	TBC	TBC
CR-013 Protective Security	25	20	↔	16	4	Limited	Apr-25
CR-014 Data Protection	20	16	↔	8	8	Limited	Jun-26
CR-015 Mailroom	25	25	↔	16	9	Insufficient	Mar-25

Current Position of Risk	
Red	10
Amber	6
Yellow	
Green	
Total	

Summary of Changes

- Register now totalling 16 risks.
- CR-008 has now been re-assessed.
- Mailroom risk most recent addition- please note mailroom is one of the 14 key business priorities for 2024-25.

Risk Heat Maps- Current vs Target Score

Current Risk Profile

Residual Likelihood	1	2	3	4	5
5					CR-011 CR-015
4			CR-005	CR-007 CR-014	CR-002 CR-003b CR-004 CR-008 CR-009 CR-010 CR-012 CR-013
3				CR-001 CR-003a CR-006	
2					
1					

Residual Impact

Target Score Profile

Residual Likelihood	1	2	3	4	5
5					
4				CR-012 CR-013 CR-015	
3			CR-006	CR-007	CR-002 CR-003b CR-004 CR-008 CR-011
2			CR-005	CR-001 CR-003a CR-014	CR-009 CR-010
1					

Residual Impact

CR-001		
Workforce planning and organisational design		**12**

Social Security Scotland must be structured to deliver a service in the most cost effective and efficient way, ensuring that our workforce is deployed flexibly to meet business needs and is developed and supported to deliver services in line with our values. Failure to manage our workforce in this way may lead to inefficient structures, processes and sub-optimal levels of productivity, leading to delays or errors in payment of benefits, undermining public confidence in the organisation and creating reputational damage with the public and stakeholders.

Current Controls:	Planned Actions:
• **Directive**: HR Business partner support for Deputy Directors; senior leadership messaging on budget approach (December 2023). • **Corrective**: Budget approach agreed for 2024-25. • **Preventative**: Finance and people working group established for oversight of staffing and budgets	• Enterprise Resource Planning still set to go live in October. • Work in progress with Finance colleagues to better control staff numbers. • Exceptions process working well, but still to strengthen information to support decision making.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
8	March 2025	4	Limited	Treat
Risk Owner		Nicola Rudnicki	Action Owner	[REDACTED]

CR-002		
Fraud		**20**

Social Security Scotland will be targeted by persons (both inside and outside our organisation, acting alone or in a group) who will seek to exploit vulnerabilities in our fraud defences for financial gain resulting in reputational damage and financial loss to the organisation.

Current Controls:

- **Preventative**: Mandatory fraud awareness sessions; Fraud and error Subject Matter Experts involved in development of delivered benefits and associated processes; Risk analysis and control officers embedded within Client Service Delivery operational sites; Fraud champions network established; BPSS check on all new colleagues joining the organisations.
- **Corrective**: Counter fraud function in place with trained specialists.
- **Detective**- Cyber defence live monitoring, public fraud reporting line in place and open.

Planned Actions:

The following will strengthen Detective Capability:

- Fraud and Error Data Layer- business launch Autumn 2024. This will improve fraud and error interventions and associated outcomes.
- July 2024- launch of the strategic fraud case management systems; August 2024 will see the old tactical solution decommissioned.
- Q3/4 check for levels of control being applied.
- [REDACTED]

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
15	April 2029	5	Limited	Treat
Risk Owner		Stephanie Glavin	Action Owner	[REDACTED]

CR-003a		
Value for money		**12**

Social Security Scotland must demonstrate that its operations secure value for money, that we are operating economically, efficiently and effectively. Failure to demonstrate this may undermine public confidence in the organisation and lead to reputational damage and public and stakeholder criticism.

Current Controls:	Planned Actions:
• **Corrective**: Performance Forum- collective leadership assessing performance risks and issues, including value for money. This provides regular updates to the Executive Team; Executive Team identified savings will be project managed; Finance Team track progress through the Finance and Investment Forum • **Directive:** Staffing Principles in place.	• Staffing principles- paper accepted by Executive Team and now implemented. • Finance and People colleagues providing a monthly resourcing/workforce planning pack to Deputy Director's so support decisions on recruitment and exceptions process.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
8	March 2025	4	Limited	Treat
Risk Owner		Stephanie Glavin	Action Owner	[REDACTED]

CR-003b		
Financial Management		**20**

Social Security Scotland must live within the Resource Spending Review settlement. This requires that we accurately forecast our future need and ensure, as far as possible, that areas spend in line with forecast. Where activity varies from forecast this may lead to reallocation of funding to support priority business activity at the expense of other areas, leading to a degradation of some Agency services with the potential to undermine parts or all of our services.

Current Controls:

- **Detective**: Regular monitoring and reporting of in-year financial position (monthly basis)**;** Financial planning function in place, mid-term financial plan prepared and updated quarterly.
- **Preventative**: Close working with workforce planning colleagues (monthly check-in); Finance business partners in place; Benefit forecasting review group in place (monthly meeting) which considers demand for spend and forecast of full year position; Director General finance forum (fortnightly meeting); Close working with SG Finance colleagues; Small working group (meeting fortnightly) to work with governance team to plan on priorities and business change.

Planned Actions:

- Transition costs- better view of what transition will look like and will be monitored through the Legacy Portfolio workstream- Quarterly meetings minimum.

[REDACTED]

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
15	April 2025	5	Substantial	
Risk Owner		Stephanie Glavin	Action Owner	[REDACTED]

CR-004		
Quality		**20**

Social Security Scotland's efficacy as a public body delivering benefits is reliant on us making the correct decisions on benefit entitlement. Without the systems and processes that both support and demonstrate accurate decision making, the level of fraud and error is likely to significantly increase, leading to increased financial loss, loss of client and public confidence and reputational damage.

Current Controls:

- **Corrective**: Latest systems releases: Mandatory classification on all over and under payments; Functionality on unapplied deductions for payment correction cases; Quality strategy of all benefits- all checks are recorded within data bases consistently and are more visible;
- **Preventative**: Carers Support and Winter Heating Payments quality data base and checking sheets in place; Line Manager checks on pre-payment and post payment checks; Intervention Error Corrections; Monetary Value of Fraud and Error Team checking official error
- **Detective**: Organisational Improvement Team discuss the errors monthly- continuous improvement approach applied to triage any improvement required

Planned Actions:

- Draft Quality framework has been shared with Deputy Director's.
- Three Lines of Defence model to be taken to Executive Team (October 2024)
- Quality Framework is part of the business plan initiatives.
- Discovery work on PCC (Payment Correction Cases) on automation work to stop over and underpayments is progressing; looking at guidance and operational structures

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
15	March 2025	5	Limited	Treat
Risk Owner		Janet Richardson and Gayle Devlin	Action Owner	[REDACTED]

CR-005		
Performance, culture and inclusion		**12**

Social Security Scotland's success is dependent on its people. We must continue to develop our performance culture in line with our values, being an inclusive service that delivers on the Charter to ensure we retain the confidence of clients and stakeholders.

Current Controls:

- **Corrective**: Targeting and attracting under-represented groups in recruitment exercises; Some manual reasonable adjustments in place where IT solutions are unavailable.
- **Detective:** Internal equality network review complete. This feeds into People services who will then pick up outputs.
- **Preventative**: Increasing the accessibility of the recruitment process; Monitor and act on Diversity data; Procurement processes amended to ensure preferred tender applications demonstrate WCAG 2.1 AA compliance.
- **Directive**: Revised Equality Impact Assessment process in place; Accessibility team in place to offer live support for impacted colleagues; Shared Services Programme Testing Lead now engaging with Change Lead to plan Social Security Involvement in User Acceptance Test

Planned Actions:

- Review of equality strategy is underway
- Project on data quality improvement underway
- Diversity objectives workbook under development
- Oracle (eHR systems) staff awareness sessions are progressing through July 2024. Queries are being collated and shared with Scottish Government Core.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
6	December 2024	6	Limited	Treat
Risk Owner		Ally MacPhail and Nicola Rudnicki	Action Owner	[REDACTED]

CR-006		
Technology and systems		**12**
As a result of Minimum Viable Outputs and tactical technical solutions from the Programme, Social Security Scotland will need to maintain a constant focus on the availability and sustainability of numerous technical components. Many of these components will add to the overall technical debt burden and potentially the continued availability of key live services (such as citizen payments) if they are not funded correctly and remediated in a timely manner.		
• Current Controls: • **Preventative**:[REDACTED] • **Corrective**: Tracking of technical debt (size and estimated value); Tracking the life cycle of technology applications with a view to future upgrades and/or replacement; Live service monitoring and service management; Back up and disaster recovery arrangements in place; Significant digital competence and capability	Planned Actions: • Digital Maturity Assessment & Investment Appraisal is being initiated and we aim to undertake procurement action later in the summer 2024 to bring on professional services	

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
9	December 2024	3		Treat
Risk Owner		Andy McClintock	Action Owner	[REDACTED]

CR-007		
Safeguarding		**16**

Social Security Scotland hold legal and moral responsibilities where concerns are identified in relation to the welfare and safety of children and adults at risk. In delivering benefits to the broader population and to those who are at risk of harm, if we do not have adequate resource, systems and processes there is a risk of serious safeguarding error, consequently resulting in serious harm or death.

Current Controls:

- **Directive**: Social Security Scotland has established a group of health and social care staff, including registered professionals; Referrals are made to the safeguarding team via the Public Protection Case Management system; Implementation of regulations has defined legislative responsibility in safeguarding.
- **Corrective**: The Safeguarding Team assess any reported potential risks of harm for a client as quickly as possible and make onward referrals to other organisations;
- **Preventative**: Dedicated team in place managing safeguarding of professionals (qualified team).
- **Detective**: Quality Support Team within Client Services Delivery- Cross agency cases- checking the standard of claims; Randomised audit in place- practice within these cases are checked for consistency

Planned Actions:

- Senior practitioners are sampling 10 cases per month to ensure consistency of decision-making.
- Business Analyst commissioned to carry out discovery work that will further inform decision-making.
- Planned actioned from Internal Audit are to be re-baselined because of the discovery work. Business Analyst discovery work continues in Safeguarding which will inform Executive Team options paper.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
12	August 2025	4	Limited	Treat
Risk Owner		Janet Richardson and Gayle Devlin	Action Owner	[REDACTED]

CR-008		
Business resilience		**20**

Without a robust and fully assured Business Continuity and Incident Management system in place, Social Security Scotland would not be able to continue delivery of its business if it was unable to respond effectively to disruptions. Failure to have a strong system would result in our inability to deliver our agreed objectives, significant financial impact and reputational damage for Social Security Scotland and Scottish Government.

Current Controls:

- **Preventative**: Incident management framework; Business continuity framework; Bi-annual exercise programme for all business continuity plans; Two corporate exercises- which can include Executive Team level for at least one exercise; Business Resilience lead attends Chief Digital Office disaster recovery exercise;
- **Corrective**: Contingency plans for specific event (e.g. industrial action).
- **Directive**: Business Resilience lead is part of Scottish Government's Cyber Security cadre; Three members of Business Resilience team have Business Continuity Institute qualification; Business training delivered to all business continuity teams across the organisation; Business Resilience team attend regular seminars/events across Scottish Government and the Business Continuity Institute; Business Resilience awareness raised through the business continuity network meetings (quarterly); Annual Business Continuity and Resilience week- participating in global initiative to raise awareness; Business resilience team are members of cross government (SG and UK Government) networks (on-going), Media training for Executive Teams (completed July 2024)

Planned Actions:

- Internal Audit Q3
- Exercises to be conducted by external parties (Police Scotland and Protective Security Centre- two separate exercises).
- Update of frameworks
- Service Design Recommendations are being progressed by project lead
- Exercised at least 25 individual business continuity plans
- Held sessions during Business Continuity awareness week (May 2024).
- New colleague emergency phone line issued.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
15	May 2026	5	Reasonable	Treat
Risk Owner		Ally MacPhail	Action Owner	[REDACTED]

CR-009		
Delivering for our clients		**20**

Acknowledging our growth and operational maturity we need to prioritise actions to sustain appropriate internal operational processes, systems, controls and performance levels to support delivery of our service. If we do not, then we risk the reputation on which we rely to secure engagement with the public and stakeholders to deliver a public service.

Current Controls:	Planned Actions:
• **Corrective**: Quality Strategy- post payment checks, and feedback look in place; Balance scorecard, Performance Forum (which provides a note to the Executive Team highlighting the current issues and related responses); Weekly Dashboards for the Chief Exec and CabSec showing performance across a range of measures (productivity, clearance times, telephony weight times etc); Appeals and Re-determination Forum (inc. Policy and legal)- audit of decision to track and support changes,	• Continuous Improvements - The work on the creation of a Continuous Improvement function across Social Security Scotland has faced considerable challenges both securing the requisite resources and agreeing across the multi-disciplinary team the scope to be taken forward. In agreement with Senior Responsible Officer and Deputy Director Sponsor the vision has been reset with the team, and steps have been taken to unblock resources with a view of this work now recommencing.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
10	December 2025	10	Limited	Treat
Risk Owner		Janet Richardson and Ally MacPhail	Action Owner	[REDACTED]

CR-010		
Cyber security		**20**

Social Security Scotland's digital systems are likely to be compromised if an effective cyber resilience environment is not built and maintained. This would lead to the loss of confidentiality, integrity and availability of digital services and/or information systems used to provide access to and delivery of devolved benefits.

Current Controls:

- **Preventative**: New head of Security Ops now in place; [REDACTED]; An updated product security checklist has been developed in conjunction with Procurement; Technical protective security controls are applied to the digital estate in line with industry best practice; Regular security assurance activities are undertaken on all Programme releases; Security assurance assessments are undertaken as part of standard procurement processes;
- **Corrective**: Vulnerability management processes enable vulnerabilities to be identified and remediated on a scheduled basis; Incident response plans are defined and regularly exercised; Technical environments monitored by a range of tools and software services.
- **Directive:** A framework of policies ensures that information and cyber security standards are defined and can be used as the basis for maintaining the organisation's cyber resilience; Standardised risk management processes are conducted to define the security risks associated with new systems, initiatives, services, and procurements; Regular collaboration occurs with the UK's National Cyber Security Centre (NCSC) and the Scottish Government's Cyber Resilience Unit.
- **Detective**: Threat intelligence tools are used to identify new or emerging threats;

Planned Actions:

- Cyber Resilience Framework internal audit progressing well. Target date for completion remains end of June 2024.
- SG are undertaking a simulated phishing exercise across SCOTS users. Approval has been given by LT for this to include Social Security Scotland. This will begin in July and will last for 10 months, with 10% of staff receiving phishing emails each month.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
10		10	Limited	Treat
Risk Owner		Andy McClintock	Action Owner	[REDACTED]

CR-011		
Programme closure		**25**

Once Social Security Programme ends, the agency must be in a position of full responsibility and accountability for its services and must have the right capability, capacity and funding to run, maintain and change those services.

Current Controls:

- **Preventative**: New strategic workforce planning team now in place; Capability and maturity mapping exercise has been undertaken to scope the size and scale of the work required.

Planned Actions:

- Full quality review of all areas to transition from Programme agreed.
- Capability maturity agreed with Exec.
- Detailed focus on live running capabilities.
- Detailed maturity assessments invoked with IT service management data, information service management and business analysis.
- Working with the Exec to understand the post-2026 landscape.

Please note change of Action Owner.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
15	April 2025	10	Insufficient	Treat
Risk Owner		Ally MacPhail	Action Owner	[REDACTED]

CR-012		
Management information and performance (data)		**20**

Social Security Scotland must generate good quality management information and performance insights of sufficient coverage and availability to effectively and efficiently manage operational delivery, track fraud and error rates, assess corporate performance, meet reporting obligations and service the needs of key external stakeholders across UK, Scottish and Local Government and the Scottish Fiscal Commission.

Failure to do so would lead to inaccurate reporting (both internal and external), hamper decision making, impact service management and not meet the needs of key stakeholders.

Current Controls:

- **Corrective**: Manual workarounds and Excel-based reporting

Planned Actions:

- Data Branch is progressing with the hiring of a new Data Quality Analyst.
- We have applied for inclusion into a Scottish government data maturity assessment cohort to better understand the data gaps. The assessment will start in September 2024 and overseen by our Data Governance and Management team
- With the new Chief Data Officer, Head of Data now in place, a finalisation of the data strategy will be completed in the next period.
- The data services team is working closely with the data programme to better understand and appropriately prioritise data quality gaps.
- Work to align master data lists continues with further analysis in progress.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
16	April 2025	4		
Risk Owner		Ally MacPhail and Andy McClintock	Action Owner	[REDACTED]

CR-013		
Protective Security		**20**

There are multiple security threats faced by Social Security Scotland including, but not limited to, sabotage, subversive action, criminal activity and acts of terrorism. A failure to have adequate and measured holistic Protective Security measures in place to deter, detect, delay, mitigate and respond could lead to the harm or compromise of Social Security Scotland staff and assets as well as adversely affect the organisation's objectives, undermine public confidence in the organisation and create reputational damage with the public and stakeholders.

Current Controls:

- **Preventative**: Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems exist; CTV, Guard Force and Security Alarm Systems are in place and act as a detective control too; Panic Alarms, Security Vetting, Security Advice/Briefing are in place; NPSA Guidance exists and is comprehensive; Insider Threat Working Group has been formed; Security awareness and culture being introduced; Critical Asset Risk Assessment has commenced.
- **Directive:** Security signage; National Security Vetting Policy mandatory; Online security training.
- **Corrective**: Security briefings currently contain reference to Counter Terrorism; Ongoing assessment of existing procedures.

Planned Actions:
A tender is in progress for security barriers.
[REDACTED]
[REDACTED]

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
16	April 2025	4	Limited	Treat
Risk Owner		Nicola Rudnicki	Action Owner	[REDACTED]

CR-014		
Data Protection		**16**
Social Security Scotland must comply with data protection legislation and policies. This includes considering how we will protect, use, share, store and delete the personal data of our staff and clients in everything we do. Non- compliance may result in material harm because of unauthorised access, sharing or loss of personal data and lead to poor client service, increased costs, inefficiencies, compensation, reputational damage and regulatory enforcement action including fines.		
Current Controls: • **Directive**: e-learning; Routine communications. • **Preventative**: Lessons learned from previous breaches; Data retention strategy; Restricted access security controls	Planned Actions:	

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
8	June 2026	8	Limited	Treat
Risk Owner		Janet Richardson, Andy McClintock and Professor Paul Knight	Action Owner	[REDACTED]

CR-015		
Mailroom		**25**

Social Security Scotland requires a mailroom that delivers a service to the organisation in an efficient and cost-effective way. Without an effective mailroom service with the proper infrastructure the organisation will fail to meet statutory obligations and published commitments which will lead to delays in client payments and reputational damage with the public and stakeholders.

Current Controls:

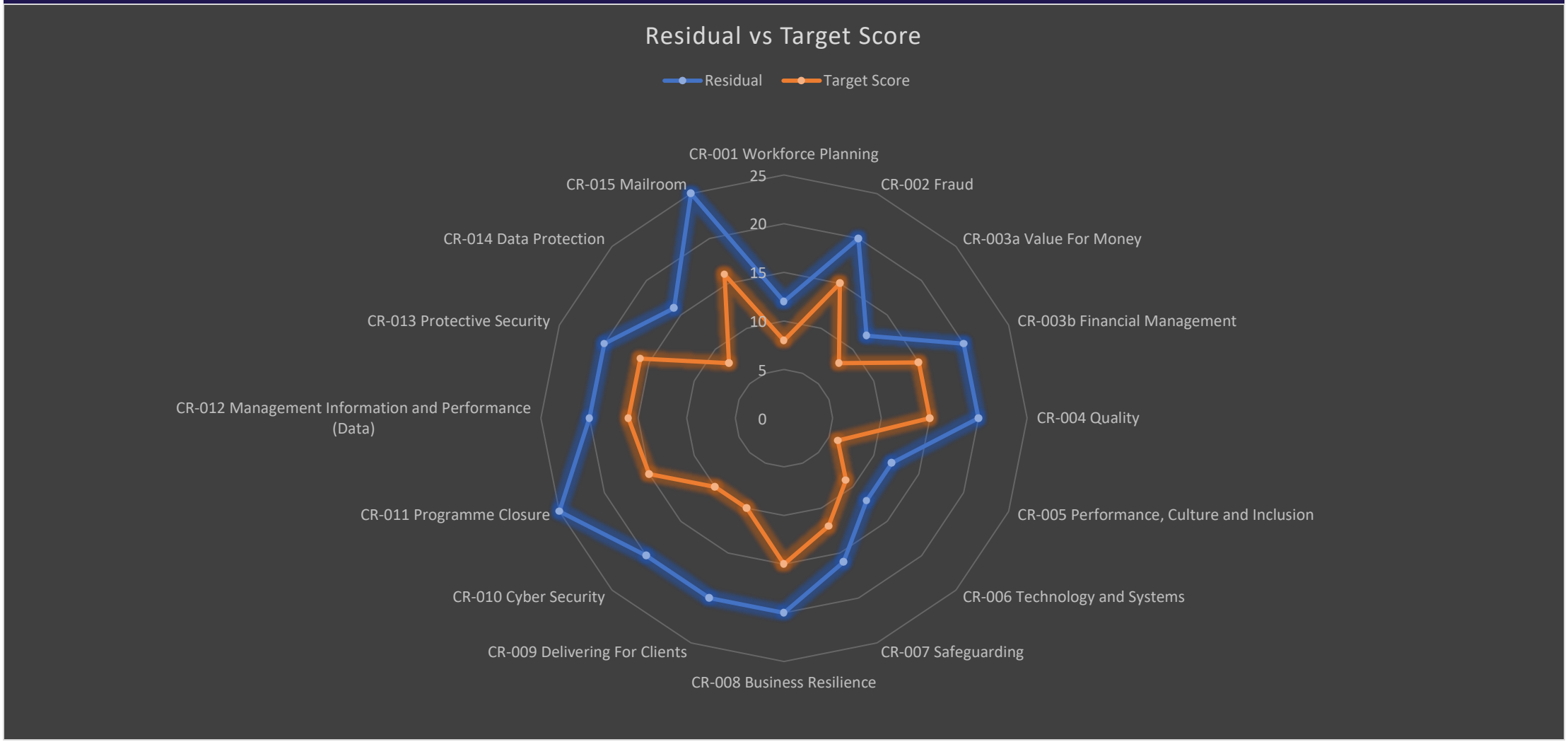
- **Corrective**: Mailroom Manager works with Finance Business Manager to monitor and control mailroom spend; Mailroom work closely with CDO Application Support team to manage system issues; User research work complete and resourcing levels meet current work expectation
- **Preventative**: Improved productivity (new scanner contract in place May 2024 to 2028);

Planned Actions:

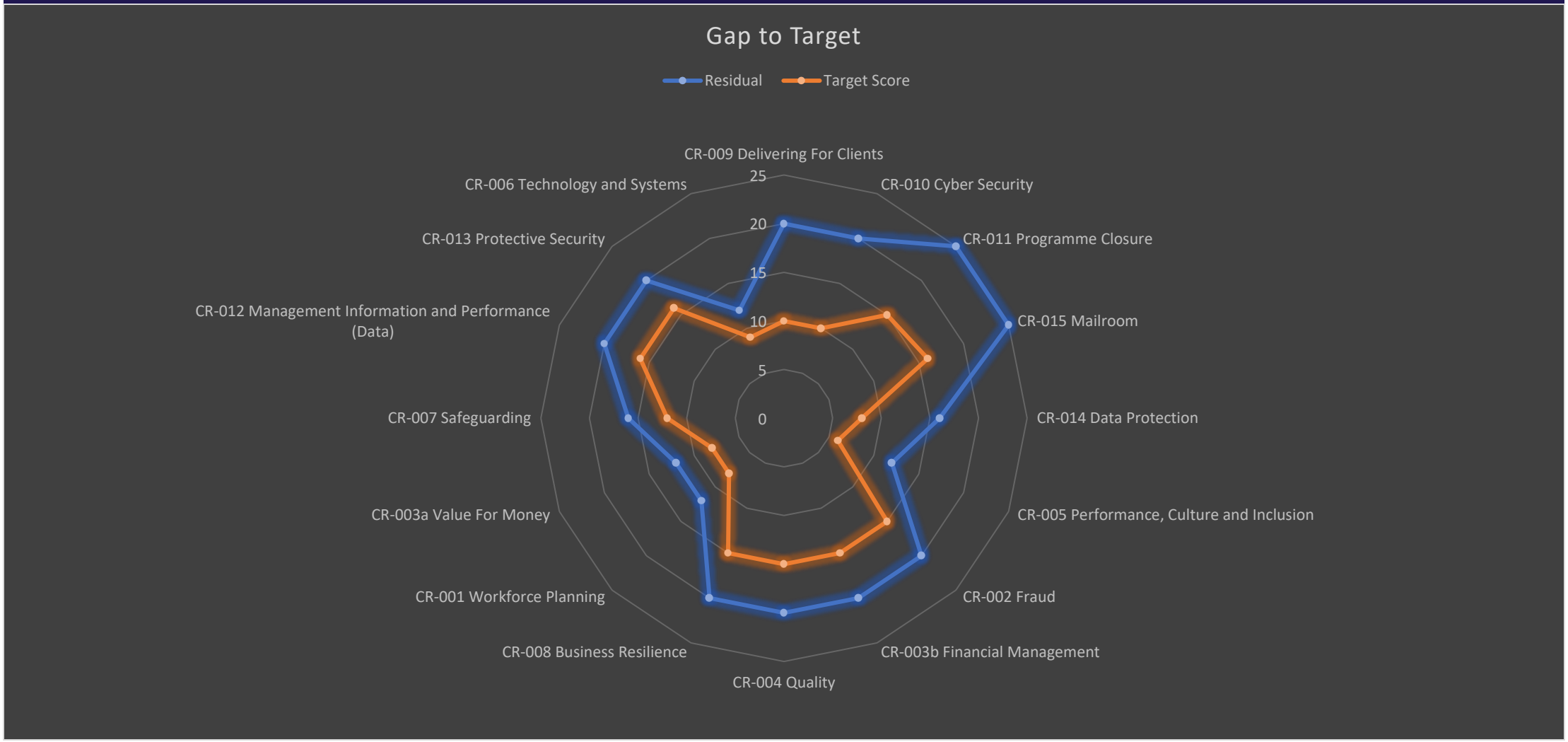
- [REDACTED]
- [REDACTED]
- Finance reports submitted and response expected August 2024
- Internal Audit finalised- awaiting sign off.

Target Score	Target Score Date	Gap To Target	Control Confidence	4T's
16	March 2025	9	Insufficient	Treat
Risk Owner		Janet Richardson	Action Owner	[REDACTED]

Overall Social Security Scotland Risk Profile



Overall Social Security Scotland Risk Profile



Top five risks by gap to target score

Risk Description	Inherent	Residual	Score Change	Target Score	Gap to target	Control Confidence	Date to target score
CR-009 Delivering For Clients	25	20	↔	10	10	Limited	Mar-25
CR-010 Cyber Security	25	20	↔	10	10	Limited	Apr-29
CR-011 Programme Closure	25	25	↔	15	10	Insufficient	Mar-25
CR-015 Mailroom	25	25	↔	16	9	Insufficient	Apr-25
CR-014 Data Protection	20	16	↔	8	8	Limited	Mar-25

Social Security Scotland
Tèarainteachd Shòisealta Alba

Risk Management Team

[REDACTED]