Social Security Scotland
Tèarainteachd Shòisealta Alba

Audit and Assurance Committee

Quarter 1-March 2025 to May 2025

Dignity, fairness, respect.

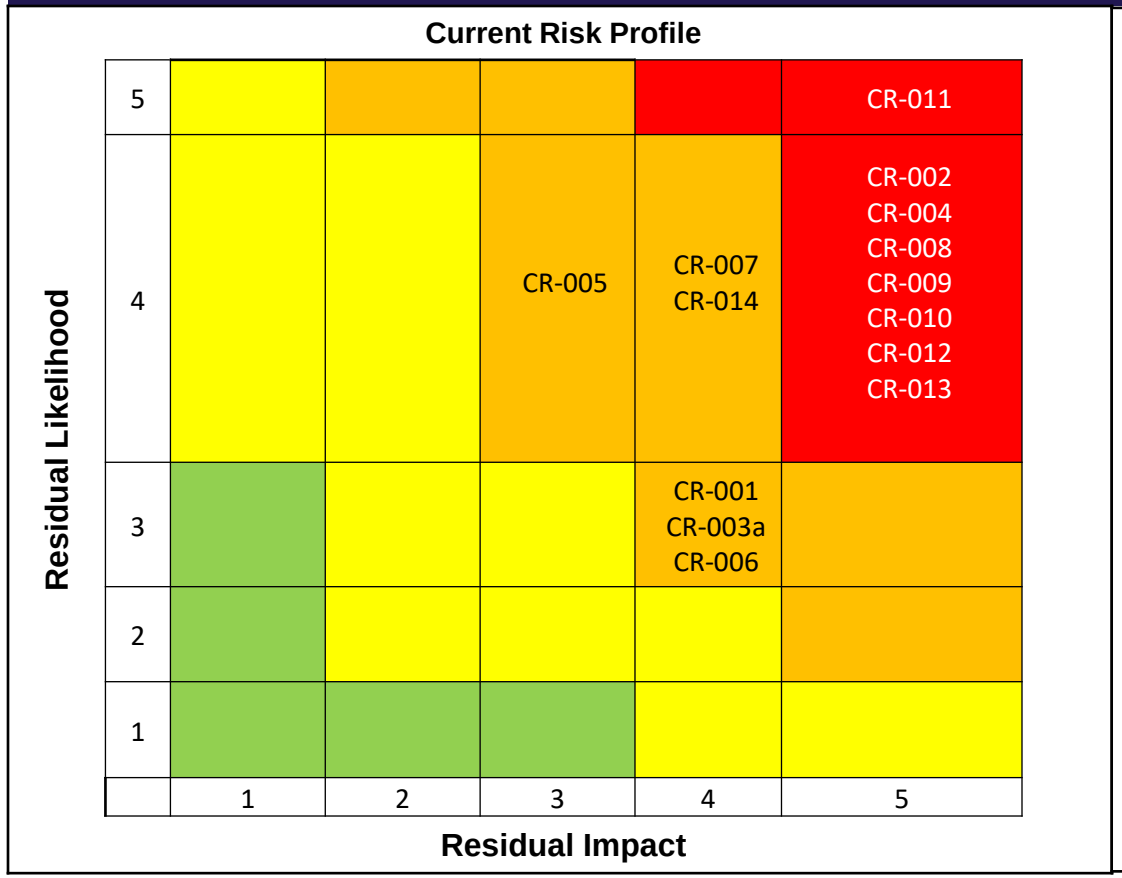
Overall Social Security Scotland Risk Profile

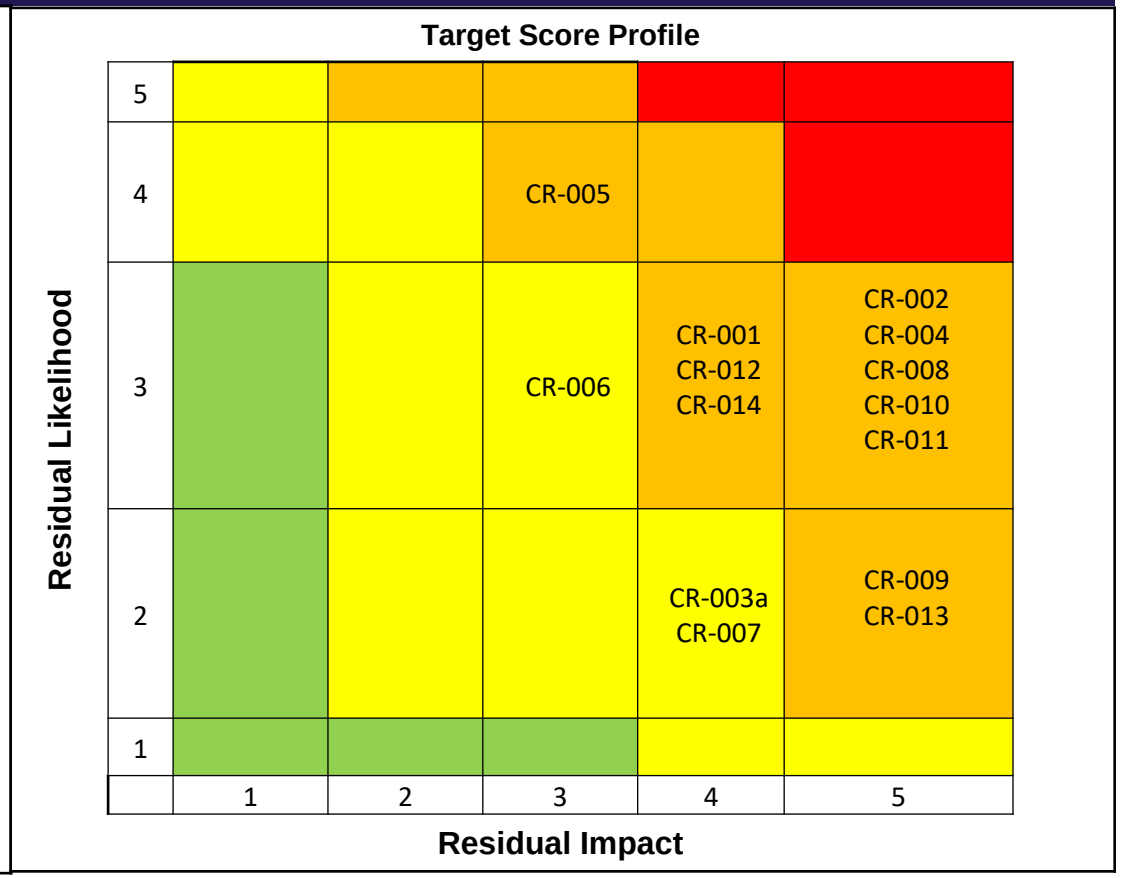
Risk Description	Risk Appetite	Inherent	Residual	Score Change	Target Score	Gap to target	Control Confidence	Date to target score
CR-001 Workforce Planning	Medium	20	12	↔	12	0	Reasonable	**Tolerate**
CR-002 Fraud	Very Low	25	20	↔	15	5	Limited	Jun-25
CR-003a Value For Money	Low	20	12	↔	8	4	Limited	**Under review**
CR-004 Quality	Low	25	20	↔	15	5	Limited	**Tolerate**
CR-005 Performance, Culture and Inclusion	Medium	9	12	↔	12	0	Limited	July-25
CR-006 Technology and Systems	Medium	16	12	↔	9	3	Limited	Dec-25
CR-007 Safeguarding	Very Low	20	16	↔	8	8	Limited	Aug-25
CR-008 Business Resilience	Very Low	25	20	↔	15	5	Reasonable	May-26
CR-009 Delivering For Clients	Low	25	20	↔	10	10	Limited	Dec-25
CR-010 Cyber Security	Very Low	25	20	↔	15	5	Limited	Aug-25
CR-011 Programme Closure	Low	25	25	↔	15	10	Insufficient	Apr-25
CR-012 Management Information and Performance (Data)	Low	20	20	↔	12	8	Limited	**Tolerate**
CR-013 Protective Security	Very Low	25	20	↔	10	10	Limited	Apr-26
CR-014 Data Protection	Very Low	20	16	↔	12	4	Limited	**Tolerate**

Risk appetite descriptors

Risk Appetite Rankings	Very Low	Low	Medium	High	Very High
	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is a key objective. Activities undertaken will only be those considered to carry virtually no inherent risk	Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk	Preference for safe options that have low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.	Eager (or required) to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

Risk Heat Maps- Current vs Target Score





CR-001 Workforce planning and organisational design

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-001	20↔	12↔	12↔	Medium	Reasonable	Tolerate

Risk Reviewed 31/03/25- remains tolerated.

Details from review:

- Agency now has a strategic workforce forum that reports to the Executive Team and is there to advice and make recommendations around work force planning related activities. Two meetings have taken place (Feb and March) and reports monthly. Work on workforce planning and the relationship with budget (affordability) will be more visible and we now have a route to Executive Team to make recommendations and manage that affordability.
- External recruitment controls- a proforma is completed and passed to central government that includes FTE and provides an extra level of scrutiny.

Next Review June 2025 will consider operating model work that is underway.

Key Controls

- HR Business Partners will be more involved with Deputy Directors (both support and challenge) to ensure decision are based on priorities.
- Combining joint finance and workforce analytic data packs for Deputy Director's and Senior Leadership Team's to give greater oversight to their staffing and budgetary positions.
- Published the Staffing Principles.

CR-002- Fraud

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-002	25 ↔	20 ↔	15↔	Very Low	Limited	June 2025

Key Controls

- Counter fraud function in place, with appropriately trained specialist colleagues.
- Pro-active data analysis with investigative and corrective function in place.
- Counter fraud function in place, with appropriately trained specialist colleagues.
- Public fraud reporting line in place and open.
- Fraud Awareness sessions are a mandatory part of induction learning.
- Risk Analysis and Control Officers are fully integrated within CSD Operational sites.
- Fraud Champion network in place.
- BPSS (Baseline Personnel Security Standard) check (or higher level of National Security Vetting depending on role) for all new colleagues joining the organisation.

Planned Action- Update

- Successful deployment of Main Release 2 (2025) for the Fraud and Error Data Layer.
- Exec Team indicated their support for Fraud and Error Investment proposed on 15/04/2025, next steps are presentation to DG Communities and then a submission and potentially meeting with the Cabinet Secretary in May and June 2025.
- Fraud and Error improvements have been prioritised in the 2025/26 Business Plan and Project Initiation Work is ongoing now – a milestone plan will be produced as part of that work and further updates will follow, as will a new Target Score Date when the next major milestone is expected.

CR-003a- Value for money

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-003a	20	12↔	8↔	Low	Limited	Under Review

Key Controls

- Savings that have been identified within areas agreed by Executive Team will be project managed; Finance track progress through the Finance and Investment Forum.
- Strategic Workforce Forum tracking efficiencies.

Planned Action- Update

- All financial risk is being re-assessed for 2025-26
- A new Financial Sustainability risk is currently being assessed to replace CR-003a and CR-003b.

CR-004- Quality

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-004	25↔	20↔	15↔	Low	Limited	Tolerate

Key Controls

- 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 the same way and are more visible.
- Organisational Improvement Team discuss the errors monthly.
- Error Control Strategy for the Agency is in place.

Planned Action- Update

- Risk has moved to tolerate until vacant posts are filled to take forward controls and re-assess the risk to reflect organisational wide quality.
- Business as usual activity remains in place.
- First review of risk 24th June to confirm new action owners and re-assess for 2025-26.

CR-005- Performance, culture and inclusion

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-005	9↔	12↔	12↔	Medium	Limited	July 25

Key Controls

- Targeting and attracting under-represented groups in recruitment.
- Internal equality network has been reviewed and is in place.
- Revised EQIA (Equalities Impact Assessment) process and guidance.
- Monitoring and act on Diversity data.
- Procurement processes amended to ensure preferred tender applications demonstrate WCAG 2.1 AA compliance ahead of contract award.

Planned Action- Update

- Performance forum re-design underway- Update expected June 2025.
- Accessibility team has been replaced with a community of practice- Update expected June 2025.

CR-006- Technology and systems

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-006	16↔	12↔	9↔	Medium	Limited	December 25

Key Controls

- 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, including the ability to record and track faults, defects and system availability.
- Back up and disaster recovery arrangements in place.
- Significant digital competence and capability .

Planned Action- Update

- Awaiting budget allocation to begin planning.
- Outcome of Digital Maturity awareness due in May 2025.

CR-007- Safeguarding

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-007	20↔	16↔	8↔	Very Low	Limited	August 25

Key Controls

- The Safeguarding Team assess any reported potential risks of harm for a client as quickly as possible and make onward referrals to other organisations.
- Quality Support Team within Client Services Delivery.
- Randomised audit in place- samples random cases from the safeguarding system and is looked at alongside escalated cases.
- Social Security Scotland has set up a group of health and social care staff that includes registered professionals.
- Referrals are made to the safeguarding team via the Public Protection Case Management (PP-CM) system.

Planned Action- Update

- Awaiting outcome of project board to begin design of new service (expected April/May 2025).

CR-008- Business resilience

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-008	25↔	20↔	15↔	Very Low	Reasonable	May 2026

Key Controls

- Incident management framework.
- Business continuity framework.
- Contingency plans for specific events.
- 40 team/branch Business Continuity plans established.
- All team/branch plans are subject to the biannual review and exercise (validation) cycle.
- Established incident management planning group.
- Annual review of the Business Continuity Management System by senior leaders within the organisation.
- Business resilience team have industry recognised Business Continuity Institute qualifications and are members of cross government (SG and UK Government) networks.

Planned Action- Update

- 1 April - Cyber/Data Loss Plan upskilling session with Executive Team.
- May - Insider Threat awareness sessions planned for Learning at Work Week.
- May – Business Continuity and Resilience Week events scheduled.
- May – Business Continuity Team quarterly network meeting.
- June – Executive Team cyber/data loss exercise scheduled.
- September – Refresh of pandemic plan.
- Oct – Fraud crisis management exercise – exact date tbc

[REDACTED]

CR-009- Delivering for our clients

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-009	25↔	20↔	10↔	Low	Limited	December 25

Key Controls

- Quality Strategy- post payment checks and feedback loop in place.
- Balance scorecard and Performance Forum reporting to Executive Team.
- Appeals and Re-determination Forum (inc. Policy and legal)- audit of decision to track and support changes.
- Single Prioritised Backlog

Planned Action- Update

- February 2025- Main Release 1 2025 Technical Release – Range of improvements and changes spanning predominately Pension Age Disability Payment, Scottish Adult Disability Living Allowance and Low-Income Benefits (LIB) including additional automated processes across LIB Benefits- Update- everything went live as expected w/c 24th Feb.
- Review to plan milestones out to target date.
- April 2025 releases complete and delivered fixes to known problems and benefits include improvements to the Scottish Courts and Tribunal Services, Pension Age Disability Benefit evidence gather, improvements to Adult Disability Payment, Child Disability Payment Best Start Grant processes.
- Future releases are planned between June and November. More details will be provided quarterly as these are implemented.

CR-010- Cyber security

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-010	25↔	20↔	15↔	Very Low	Limited	August 25

Key Controls

- Vulnerability management processes enable vulnerabilities to be identified and remediated on a scheduled basis.
- Event logging, monitoring, alerting, and investigating is continually undertaken to identify and resolve any suspicious activity related to cyber security.
- Security assessments of key suppliers and/or systems are being completed on a prioritised basis with risks identified and action plans agreed.
- Threat intelligence tools are used to identify new or emerging threats and to inform the selection and configuration of protective controls and activities.
- Incident response plans are defined and regularly exercised.
- Technical protective security controls are applied to the digital estate in line with industry best practice and cyber security frameworks.
- An updated product security checklist has been developed in conjunction with Procurement and will be included in all relevant procurements to conduct security assessments.

Planned Action- Update

- No update in last quarter.

CR-011- Programme closure

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-011	25↔	25↔	15↔	Low	Insufficient	April 25

Key Controls

- Governance structure
  - Change and Digital Delivery Group in place escalates into Future Operating Model Senior working group.
  - Future Operating Model Senior working group (has oversite has over everything- ensure that everything is coming together across Operations, Digital and Corporate).
  - Future Operating Model Senior working group reports into the Agency Exec

Planned Actions-Update

- The high-level change and digital delivery model has been signed off and socialised across the organisation.
- Leaders across Social Security Scotland and Programme have been aligned to capabilities within the digital, change and delivery model and they are no progressing to development of lower-level designs with support from the project team (Due for completion 5th May 2025).
- Finance and People stakeholders are aligned to implementation workstreams to support model costs and people implementation impacts.

- **Key Milestones**
  - **22nd May** - Lower-level design exec sign off (Model, cost, detailed implementation plan)
  - **Jun 25** - Digital, Delivery & Change model full implementation begins
  - **Jul 25** - Leadership roles within model appointed
  - **Sep 25** - Governance structure formal approval
  - **Sep 25** - New Digital, Delivery & Change structure in place, Social Security Scotland structure in place
  - **Oct 25** - People appointments conclude

CR-012- Management information and performance (data)

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-012	20↔	20↔	12↔	Low	Limited	Tolerate

Key Controls

- Manual workarounds and Excel-based reporting: Systems were built for operational needs and therefore leads to complexity for reporting.
- Analysis and Insight team produce daily and monthly reports to key operational and executive stakeholders to enable performance management.
- Data Management Control Framework- this ensures Social Security Scotland produce high quality data including management of lists, framework for standardisation of data and critical data tables.

Planned Action- Update

- Risk has moved to tolerate until such time as business planning is completed and review of the risk will take place July 2025.
- Single data distributor is still in planning with June 2026 as the estimated delivery period.
- Data Sync is scheduled for August 2025.

CR-013- Protective security

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-013	25↔	20↔	10↔	Very Low	Limited	April 26

Key Controls

- NPSA Guidance exists and has been drawn upon to address incidents.
- Procedures have been introduced for staff to follow when it comes to issues that are either security focused or relate to security.
- CCTV, Guard Force, Security Alarm System and panic alarms are in operation.
- National Security Vetting Policy and the requirement for clear direction on the way forward with respect to vetting and vetting requirements from UK Gov and Core SG.
- Insider Threat Working Group continues developing plans and processes to address the insider threat and this is a collaborative work in progress across the Agency.

Planned Action- Update

- New procurement contract requirement for BPSS (Baseline Personal Security Standard- includes identity, employment history, right to work in UK and criminal record check) has been accepted and finalised in coordination with SG SBC and SSS Procurement.

CR-014- Data protection

Risk ID	Inherent Risk Score	Residual Risk Score	Target Risk Score	Risk Appetite	Control Confidence	Target Score Date
CR-014	20↔	16↔	12↔	Very Low	Limited	Tolerate

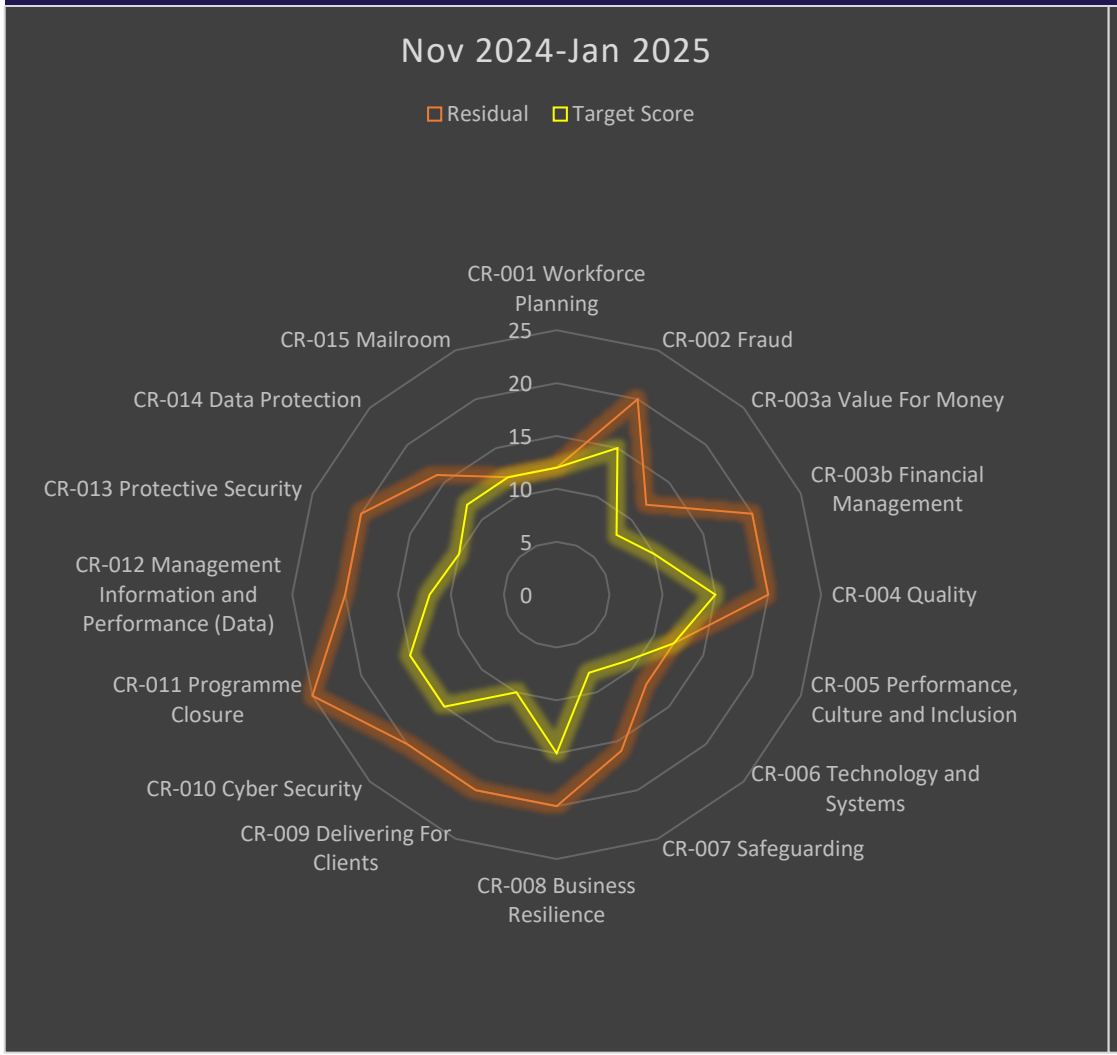
Key Controls

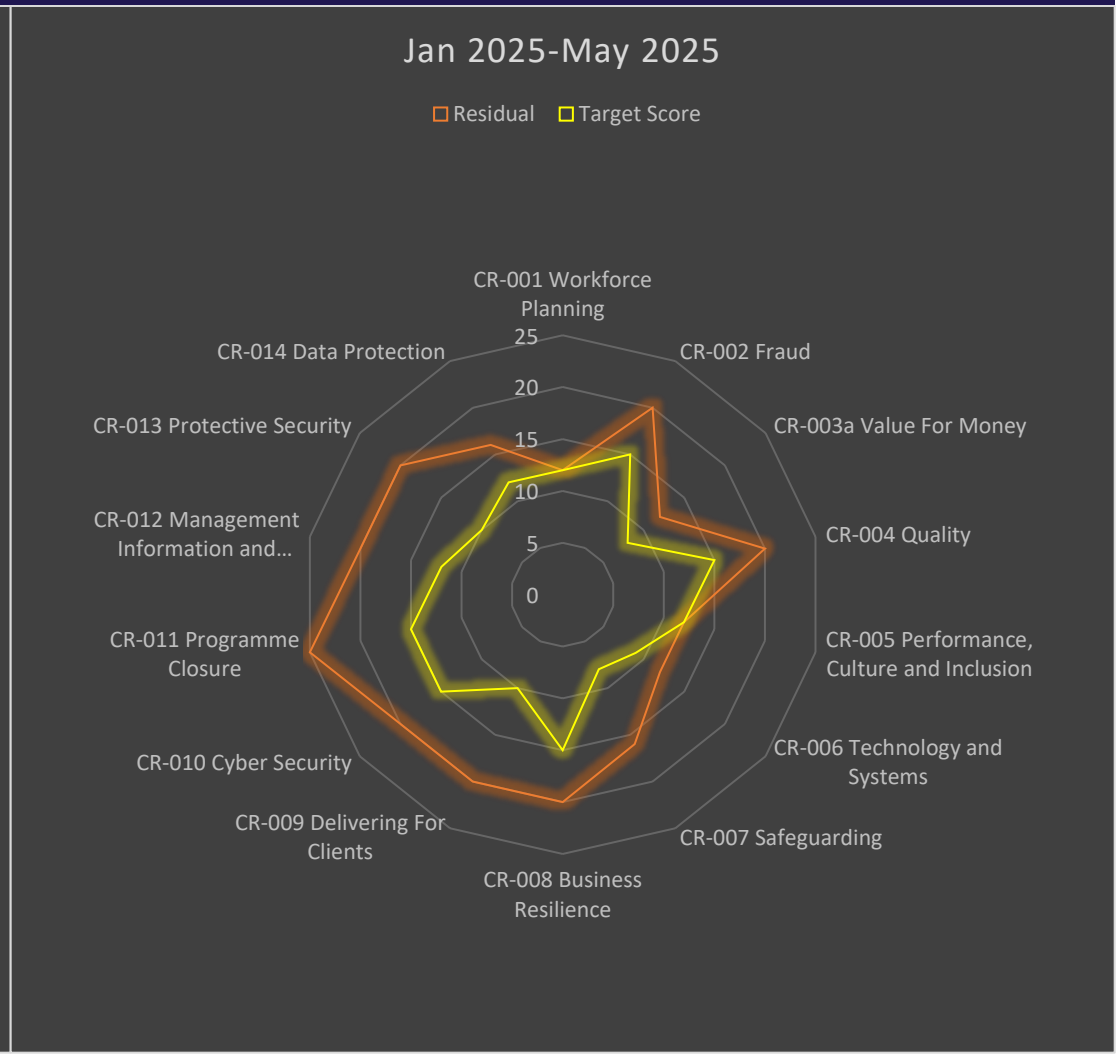
- e-learning.
- Routine communication.
- Lessons learned from previous breaches.

Planned Action- Update

- Tactical controls are in place for existing benefits and are effective. The introduction of new benefits later this year may impact that efficacy and therefore possibly increase the score in future. There are no detailed plans in place from which milestone dates can be created to demonstrate progress to the target score by the target date at this time. There is, however, a clear understanding of the work required to implement strategic controls, but since resources are operating in a reactive mode at this time, there are no firm milestones to report yet. Considering the current position, it was agreed that this risk is being tolerated.

Overall Social Security Scotland Risk Profile Comparison





Risk ID	Risk Description
CR-001	Security Scotland must operate cost-effectively and efficiently, ensuring a flexible workforce to process applications and requests swiftly and accurately, aligned with our values. Ineffective workforce management could lead to delays, client difficulties and reputational damage (undermining public confidence).
CR-002	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 financial loss to the organisation, erosion of trust Scottish Citizens place in Social Security Scotland to administer funds responsibly, and potential for increased stigma associated with claiming assistance negatively impacting our clients.
CR-003a	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.
CR-004	Consistent, accurate benefit decisions are vital to Social Security Scotland's efficiency and reputation. Without proper systems, processes, and training, errors and fraud may rise, eroding client and public confidence.

Risk ID	Risk Description
CR-005	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.
CR-006	There is a risk that essential digital services may fail and as a consequence have an impact on our clients. This could range from minor inconvenience such as information being temporary unavailable to more serious impacts such as late or missed payments or no digital access to outcome decisions. The digital estate was constructed iteratively as part of a multi-year programme, it contains significant technical debt and some tactical solutions. Social Security Scotland will need to maintain a constant focus on the availability and sustainability of numerous technical components
CR-007	Social Security Scotland are viewed as responsible for serious harm of a client due to an under/over payment, inappropriate sharing of data or in failing to recognise vulnerability and take appropriate action.
CR-008	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.

Risk ID	Risk Description
CR-009	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 to our clients. 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.
CR-010	Social Security Scotland's digital systems are likely to be compromised if an effective cyber resilience environment is not built and maintained. This could lead to client data being disclosed or corrupted with interruptions to digital services ranging from minor inconvenience to more serious impacts such as late / missed payments or the inability to make digital outcome decisions.
CR-011	Once Social Security Programme ends, Social Security Scotland 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. Without these elements in place Social Security Scotland will be at risk of not being able to monitor and maintain the current level of service over time. If this risk was to materialise there is also the likelihood of client service deteriorating over time as Social Security Scotland would not be able to carry out sufficient continuous improvement or prioritise, manage and implement change to ensure that client service can improve in line with organisational and ministerial priorities

Risk ID	Risk Description
CR-012	For our clients to trust Social Security Scotland with their personal information, we must demonstrate good data governance through trusted, timely, management information and performance insights. Internally, underpinning an efficient and timely service for our clients while externally providing visibility and accountability to both clients and government bodies. Without trusted MI driving operations or demonstration of good external governance and accountability, trust and reputation are eroded. Decision making is hampered, impacting service management and the needs of our key stakeholders. In this respect, the quality and completeness of our core data is therefore a recognised risk.
CR-013	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. These activities include the protection of client data, protecting hard copy client information received and processed by the Agency as well as ensuring the safety of both clients and colleagues during interactions both within our buildings and during off site visits. Vulnerabilities and shortfalls in such security aspects have the potential to adversely affect the organisation's objectives, including delivery of benefits, undermine public confidence in the organisation and create reputational damage with the public, clients and stakeholders alike.

Risk ID	Risk Description
CR-014	To ensure we use personal data appropriately and to protect them from harm, 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 clients and staff in everything we do. Non-compliance may result in distress or financial harm to our clients and staff because of unauthorised access, sharing or loss of personal data. In addition, our clients' and staffs' experience, and their confidence in the organisation, would be diminished. As an organisation we could also see increased costs, inefficiencies, compensation, reputational damage and regulatory enforcement action including fines.

Social Security Scotland

Tèarainteachd Shòisealta Alba