Social Security Scotland
Tèarainteachd Shòisealta Alba

Audit and Assurance Committee

Quarter 3- August 2024 to November 2024

Dignity, fairness, respect.

Overall Social Security Scotland Risk Profile

Risk Description	Risk Appetite	Inherent	Residual	Score Change	Target Score	Gap to target	Control Confidence	Proximity to Target Date (Months)	Date to target score
CR-001 Workforce Planning	Medium	20	12	↔	8	4	Limited	5	Mar-25
CR-002 Fraud	Very Low	25	20	↔	15	5	Limited	54	Apr-29
CR-003a Value For Money	Low	20	12	↔	8	4	Limited	5	Mar-25
CR-003b Financial Management	Low	25	20	↔	15	5	Substantial	6	Apr-25
CR-004 Quality	Low	25	20	↔	15	5	Limited	5	Mar-25
CR-005 Performance, Culture and Inclusion	Medium	9	12	↔	6	6	Limited	2	Dec-24
CR-006 Technology and Systems	Medium	16	12	↔	9	3	Limited	2	Dec-24
CR-007 Safeguarding	Very Low	20	16	↔	12	4	Limited	10	Aug-25
CR-008 Business Resilience	Very Low	25	20	↔	15	5	Reasonable	19	May-26
CR-009 Delivering For Clients	Low	25	20	↔	10	10	Limited	14	Dec-25
CR-010 Cyber Security	Very Low	25	20	↔	15	5	Limited	10	Aug-25
CR-011 Programme Closure	Low	25	25	↔	15	10	Insufficient	6	Apr-25
CR-012 Management Information and Performance (Data)	Low	20	20	↔	16	4	Limited	17	Mar-26
CR-013 Protective Security	Very Low	25	20	↔	16	4	Limited	6	Apr-25
CR-014 Data Protection	Very Low	20	16	↔	8	8	Limited	20	Jun-26
CR-015 Mailroom	Low	25	25	↔	16	9	Insufficient	5	Mar-25

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

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-010 CR-011
2			CR-005	CR-001 CR-003a CR-014	CR-009
1					

Residual Impact

CR-001 Workforce planning and organisational design	Tolerance	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:

Corrective

• Budget approach agreed with Workforce Planning 24/25- lessons learned are being used from previous years.

Directive

• HR Business Partners will be more involved with Deputy Directors (both support and challenge) to ensure decision are based on priorities

• Senior leader messaging issued w/c 18th December regarding budget approach

• Combining joint finance and workforce analytic data packs for DD's and SLT's to give greater oversight to their staffing and budgetary positions. This will enable and encourage effective staffing decisions. These will be ready from August onward. Workforce analytics have completed a piece of work on assumptions to allow more accurate forecasting

• Published the Staffing Principles

• Published spending now released

Planned Actions: **Risk to be reviewed 28th November 2024**

28/10/24- No update.

23/09/2024

- Approach to Performance continues to be cascaded across Agency and a plan for delivery across all functions for the remainder of 2024/25 has been agreed with Executive Team.
- Introduction of Oracle Cloud from 01/10/2024 will hopefully provide opportunities for greater control over Agency FTE and Workforce Planning (Review Nov 2024).

26/08/2024:

-The approach to performance is being cascaded across the organisation and is having an impact in terms of productivity, performance and efficiency. Activity is focused in operational areas and People and Places. This will continue to be cascaded throughout the org during this financial year.

-A key outcome is that Finance and People will jointly provide DDs with a Resourcing/Work Force Planning pack each month to better inform their divisional decisions regarding recruitment and exceptions. This is under development and a meeting with DDs Finance & Corporate Services and People & Place.

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

CR-002 Fraud	Tolerance	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:

Corrective:

• Counter fraud function in place, with appropriately trained specialist colleagues.

Detective:

• Cyber defence in place, live monitoring.
• Counter fraud function in place, with appropriately trained specialist colleagues.
• Public fraud reporting line in place and open.

Directive

• Fraud Awareness sessions are a mandatory part of induction learning.
• Fraud and Error Subject Matter Experts have been involved in development of delivered benefits and associated processes where advice on appropriate controls to mitigate against fraud risk suggested. This comes with the caveat that Fraud &Error Subject Matter Experts are one stakeholder in Programme/Agency wide discussions with competing priorities where advice is provided but not always implemented in final design and delivery.
• Risk Analysis and Control Officers are fully integrated within CSD Operational sites providing bespoke support in cases where fraud and/or error doubt has arisen.
• Fraud Champion network which empowers Operational colleagues to support each other and provides a “direct line” to the Risk Analysis and Control team.
• BPSS check (or higher level of National Security Vetting depending on role) for all new colleagues joining the organisation.

Planned Actions: **Risk to be reviewed 20th November 2024**

07/10/24

- Fraud and Error Data Layer investment case is in development.

Target Score	Target Score Date	Gap To Target	Control Confidence	Risk Appetite	4T’s
15	April 2029	5	Limited	Very Low	Treat
Risk Owner		Stephanie Glavin	Action Owner	[Redacted]	

CR-003a Value for money	Tolerance	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:

Corrective

• Collective leadership that assesses performance risk and issues; including value for money. This then provides updates Executive Team; fortnightly

• Performance Forum-Savings that have been identified within areas agreed by Executive Team will be project managed; Finance track progress through the Finance and Investment Forum

• Performance Forum- collective leadership that assesses performance risk and issues; including value for money. This then provides updates Executive Team; fortnightly

• Savings that have been identified within areas agreed by Executive Team will be project managed; Finance track progress through the Finance and Investment Forum

Preventative

• Staffing Principles are now in place.

Planned Actions: **Risk to be reviewed 12th December 2024**

No update in October 2024

24/09/2024

- Approach to Performance continues to be cascaded across Agency and a plan for delivery across all functions for the remainder of 2024/25 has been agreed with Executive Team.
- Recruitment controls and Staffing Principles continue to be implemented across the Agency
- Introduction of Oracle Cloud from 01/10/2024 will hopefully provide opportunities for greater control over Agency Full-Time Equivalent and Workforce Planning.
- Further communication around spending controls has been publish - FAQ's and Guidance has been released.

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

CR-003b Financial Management	Tolerance	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:

Corrective:

• Finance and Investment Forum reviews all business cases for existing renewal or new developments.

• Link financial and business plan

Detective:

• Regular monitoring and reporting of in-year financial position (monthly basis)

Directive:

• Financial Planning Function in place with a mid-term financial plan prepared and regularly updated (quarterly basis)

Preventative:

• Director General Finance Forum (Fortnightly meeting)

• Close working with Scottish Government Finance colleagues on arrangement for resource spending reviews (annual cycle as linked to budget).

• Close working between Finance and Workforce Planning colleagues and analysts- workforce plans and staffing requirements (monthly basis)

• Finance and Investment Forum reviews all business cases for existing renewal or new developments.

• Submission of robust data and evidence to centre to support request for budget

• Link financial and business plan

Planned Actions: **Risk to be reviewed 18th November 2024**

-11/10/24- Note from Action Owner: [Redacted]

30/08/24:

Scottish Government has introduced emergency spending controls that means some of our budget will not be spent in the way we had envisaged if it doesn't fit the essential spend category. We are giving back budget that we have not spent this year because of this and due to the Oracle freeze.

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

CR-004 Quality	Tolerance	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; this produces automated management information for official error vs client error and routine maintenance

•Functionality on unapplied deductions for payment correction cases. This functionality allows these errors to be corrected; this functionality allows Client Services Delivery and Interventions staff to reduce overpayment by underpayment or vice versa

•Quality strategy of all benefits- all checks are recorded within data bases the same way and are more visible. Individual feedback is available and can be provided to staff

Detective:

Organisational Improvement Team discuss the errors monthly- continuous improvement approach applied to triage any improvement required

Directive:

•Error Control Strategy for the Agency is in place- has been refreshed and published (May 2024)

Preventative:

•Carers Support and Winter Heating Payments quality data base and checking sheets have been launched: 100% check in place (prior to payment) until satisfaction of quality (for Carers the 100% check will stay in place and Winter Heating Payment will be reviewed after 3 months)

•Quality strategy of all benefits- all checks are recorded within data bases the same way and are more visible (team managers can access the checks that have been performed). Individual feedback is available and can be provided to staff

Current checks providing control :

• Line Manager checks- pre-payment (prevent); post payment checks (corrective);

• Intervention Error Corrections (corrective);

• Monetary Value of Fraud and Error Team- checks went live Summer 23 on Scottish Child Payment (0.8% official error detected) 30/04/24- Four new members joined Quality and Performance team improving checks for full end to end journey (detective).

Planned Actions: **Risk to be reviewed 14th November 2024**

24/09/24

- Quality Framework has completed second Quality Review, now with Deputy Director for Organisational Strategy and Performance, before going to Executive Team for sign off.
- Three Lines of defence is maturing: slot on Three Lines of Defence with the joint executive team on the 23rd October. Presenting current model and how to address the main issue identified which is the lack of ownership and accountability for driving change and improvement where issues are identified in relation to benefit delivery. Papers due 17th October (Update November).
- October Release- Auto Suspension from Date Death should reduce over payments (October 2024).

27/08/24

-Quality Framework is out for review to Strategy and they are taking forward the second phase of that business. This will include the appointment of the Business Analyst.

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

CR-005 Performance, culture and inclusion	Tolerance	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

• Internal equality network has been reviewed and is in place (network provides peer support, raises awareness across protected characteristics, supporting enabling teams to fulfil the organisations equalities obligations and embed intelligent kindness and culture activity across the organisation

Detective

• Internal equality network has been reviewed and is in place (network provides peer support, raises awareness across protected characteristics, supporting enabling teams to fulfil the organisations equalities obligations and embed intelligent kindness and culture activity across the organisation

• Some manual reasonable adjustments in place, for example additional colleague support, where IT solutions are unavailable.

• Performance Forum has been established with Gayle Devlin as sponsor (December 2023)- Executive Team sub-group. This forum meets monthly to discuss balance score and performance.

Directive

• Revised EQIA process and guidance is now on Saltire. Pathways learning is also live and a presentation was delivered to the weekly leadership team on 2 July. D&I Team are running sessions with other groups across the organisation to raise awareness and offering regular learning sessions and support

• Accessibility Team has been stood up on 22/05/2023 to create holistic strategy to build accessibility into design processes, governance and assurance as well as other best practice advice, guidance and processes

• Accessibility team in place to offer live support for impacted colleagues, reducing impact on their inability to carry out roles due to barriers, escalate technical issues for prioritisation on single prioritised backlog

• Shared Services Programme Testing Lead now engaging with our Change Lead to plan Social Security Involvement in User Acceptance Test

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 ahead of contract award (there are stipulations for undue burdens etc).

Planned Actions: **Risk to be reviewed 9th December 2024**

16/10/2024:

-New Oracle HR System live from 7th October 2024. Minor errors being tracked but the risk score will remain the same as these errors are minor and do not increase the score. Update in November will give a better picture of control.

10/09/2024:

- Developing Pathway to Inclusion tool to assist colleagues to develop their mandatory Diversity and Inclusion objective from April 2025.

13/08/27:

-Performance and Quality framework development started (Performance Equality Framework for Benefits by end of Dec 2024)

- Impact of Oracle will be assessed once it goes live (Oct 2024)

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

CR-006 Technology and systems	Tolerance	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:
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, including the ability to record and track faults, defects and system availability (help desk) (Corrective/Preventative).
• Back up and disaster recovery arrangements in place
• Significant digital competence and capability
Preventative
• [Redacted]
• [Redacted]
• Tracking the life cycle of technology applications with a view to future upgrades and/or replacement systems
Significant digital competence and capability

Planned Actions: **Risk to be reviewed 12th November 2024**
16/10/24
-Approval given for a Digital Maturity Assessment. Procurement initiated and Invitation to Tender issued to circa. 9 potential suppliers. Tender closes at end of October with a Target contract award date of 22 November. All works specified to be complete by end of March 2025 to be undertaken with outputs complete by the end of March 2025
22/08/24:
-Control confidence set to Limited- awaiting approval of a Digital Maturity Assessment of the digital estate.

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

CR-007 Safeguarding	Tolerance	16

Social Security Scotland hold 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:

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, such as the relevant local authority, as appropriate.

Detective

• Quality Support Team within Client Services Delivery- Cross agency cases- checking the standard of claims made and independent checks of 'post events' including checking if safeguarding has been applied or was appropriate.

• Randomised audit in place- samples random cases from the safeguarding system and is looked at alongside escalated cases (most complex cases; e.g. high value payments, addiction services, child protection)- practice within these cases are checked for consistency

Directive

• Social Security Scotland has set up a group of health and social care staff that includes registered professionals, e.g. social workers who have previous experience in handling cases which involves child and adult protection.

• Referrals are made to the safeguarding team via the Public Protection Case Management (PP-CM) system. Guidance and procedures are in place to support client facing colleagues to raise safeguarding concerns via PP-CM.

• Implementation of regulations (16th January) increased responsibility to organisation- defined legislative responsibility in safeguarding

Preventative

• Dedicated team in place managing safeguarding of professionals (qualified team)

Planned Actions: **Risk to be reviewed 8th November 2024**

29/10/24

- awaiting outcome from options paper to Executive Team on 5th November 2024.

09/10/2024

- Business continuity and Incident management framework endorsed by the Exec Team.
- Service Design Recommendations are being progressed by project lead - still ongoing.

01/10/24

- Internal Audit recommendations have been reviewed and have informed the discovery work.
- Initial project board took place w/c 23rd September with Senior Leaders across the agency. Discover report to be delivered to the project board on 22nd October- makes a number of recommendations for Executive Team to implement; comparing the need for service design and immediate solution requirement. This will work towards establishing controls.
- Broader local delivery work to look at "appointee issue"- divisional level risk and issue raised and linked to strategic risk.
- Upcoming launch of Pension Age Disability Payment potential additional demand on safeguarding (Pilot October 2024- Review November).

03/09/24

- Business Analyst in place with a business architect, service designer and project team undertaking discovery work on Safeguarding needs which has regular checkpoints for overview and decision making at ET level and project board oversight- they will be scoping out solutions that will bring appropriate controls to delivery; First checkpoint will be 4th September (monthly checkpoints) to discuss plans with more substantial update in October 2024.

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

CR-008 Business resilience	Tolerance	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:

Planning

- Incident management framework (**Preventative**)
- Business continuity framework (**Preventative**)
- Contingency plans for specific event (e.g. industrial action) (**Corrective**)
- 30 Business Continuity plans have been exercised (**Corrective**)

Exercises

- Bi-annual exercise programme for all business continuity plans across the organisation that all business continuity teams attend (**Preventative**)
- Two corporate exercises- which can include Executive Team level for at least one exercise (e.g. two cyber security exercises were run during 2023-2024)- (**Preventative**)
- Business Resilience lead also part of Scottish Government's Cyber Security cadre (**Directive**)
- Business Resilience lead attended Chief Digital Office disaster recovery exercise (**Preventative**)

Training

- Three members of Business Resilience team have Business Continuity Institute qualification and provide subject matter expertise (**Directive**)
- Business Resilience team have delivered training to all business continuity teams across the organisation (**Directive**)
- Business Resilience team attend regular seminars and events across Scottish Government and through the Business Continuity Institute (**Directive**)
- Media training for Executive Teams completed July 2024 (**Directive**)
- Awareness and culture (**Directive**)
- Business Resilience team raise awareness throughout the year on business continuity through on-line events and communication activity (e.g. newsletters and line manager cascades)- (**Directive**)
- Awareness also raised through the business continuity network meetings (quarterly) with the teams in place across the organisation (**Directive**)
- Annual Business Continuity and Resilience week- participating in global initiative to raise awareness (**Directive**)
- Annual review of the Business Continuity Management System by senior leaders within the organisation; Executive Team are provided with output (**Corrective**)
- Business resilience team are members of cross government (SG and UK Government) networks (on-going) (**Directive**)
- Colleague emergency line has been launched (**Directive**)

Planned Actions: **Risk to be reviewed 19th November 2024**

14/08/24

- Police Scotland exercise October 2024
- Security Exercise September 2024 (Protective Security Centre)
- An internal audit of the business resilience function is scheduled for Quarter 3 of this financial year.
- Multi-agency exercise lead by business resilience and facilitated by Police Scotland – scheduled for October 2024
- Officer in Charge (OIC) review paper to be taken to Executive Team – date tbc
- Larger scale mailroom exercise to be planned between business resilience and mailroom colleagues, involving security, place services and others
- Security escape room sessions arranged by Business Resilience, facilitated by SG security colleagues – due in September across both sites in AHH/GHS
- Executive team cyber related session scheduled for October 2024. Planning underway between resilience and cyber colleagues

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

CR-009 Delivering for our clients	Tolerance 10-15	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:

Assurance for Business as Usual

•Quality Strategy- post payment checks and feedback loop in place (**Corrective**)

•Quality Strategy- post payment checks and feedback loop in place (**Corrective**)

Measurements of performance

• Balance scorecard, Performance Forum (provides a note to ET highlighting the current issues and responses to issues); Weekly Dashboards for the Chief Exec and CabSec showing performance across a range of measures (productivity, clearance times, telephony weight times etc); (**Corrective**)

Feedback

• Appeals and Re-determination Forum (inc. Policy and legal)- audit of decision to track and support changes (**Corrective**)

Planned Actions: **Risk to be reviewed 25th November 2024**

22/10/24-

Delivery Plan Initiatives:

-Phase 1 of mailroom and notification improvements for staff, clients and financially are being taken forward to delivery. Phase 2 to consider remaining action.

-Discovery activity in flight- safeguarding, local services (process, resources, job roles etc.)- Safeguarding ends October 2024, Local Services will run to December 2024 (possibly beyond).

-Work on Quality and Performance framework- green for the purposes of delivery- Reported to ET completed phase 1 drafted and being Quality Reviewed- moving on to quality measures and performance measures.

-Fraud and Error work- devising the future investment case for Fraud and error which is expected to be signed off with the governance forum (in finance mode) by March 2025. Commission for project resource will be required to support implementation (Discovery and what the requirements will be (internal controls)).-Operational Delivery improvements- [Redacted] will go back to the Finance Forum in October. Pending approval will give another 3 months of support, [Redacted]

-Change Improvements (CI) blocked since start of September- RED rag status- [Redacted]. Business analysts and architects are working on this model. [Redacted]. Assessment of requirements presented to ET in September, and no decision was given- further due diligence was asked for with Programme. The resource is not available through Programme and more discussions to had during October. Hopefully this will then be unblocked.

The challenge for Change Improvements: [Redacted].

Delivery of the business plan:

-As written, a lot is being done to sustain internal operational processes, systems and performance. (Prioritized element of this risk needs to be improved).

For CR-009

-Client Service Delivery- providing control on training, performance and feedback

-Project Management Office- providing strategic control and improvement control

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

CR-010 Cyber security	Tolerance	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:

Corrective

- 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 (new October 2024).

Detective

- 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 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

Preventative

- New head of Security Ops now in place
- [Redacted]
- An updated product security checklist has been developed in conjunction with Procurement and will be included in all relevant procurements to conduct security assessments (Preventative).
- Technical protective security controls are applied to the digital estate in line with industry best practice and cyber security frameworks
- Regular security assurance activities are undertaken on all Programme releases to ensure ongoing security by design standards are applied to all systems used to deliver benefits
- Security assurance assessments are also undertaken, where relevant, as part of standard procurement processes
- Event logging, monitoring, alerting, and investigating is continually undertaken to identify and resolve any suspicious activity related to cyber security
- Incident response plans are defined and regularly exercised
- Technical environments monitored by a range of tools and software services
- Improved processes around access management and privileged accounts have been implemented and enforced (New October 2024).
- Implementation of improved vulnerability management processes which triage, assess and classify new vulnerabilities based on actual risk (new October 2024)

Planned Actions: **Risk to be reviewed 13th November 2024**

30/10/24

- Cyber security awareness sessions were provided to the Executive Team and Executive Advisory Body [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

22/08/24

- [Redacted]
- SG simulated phishing exercise across SCOTS users- [Redacted]

Target Score	Target Score Date	Gap To Target	Control Confidence	Risk Appetite	4T's
15	August 2025	5	Limited	Very Low	Treat
Risk Owner		Andy McClintock	Action Owner	[Redacted]	

CR-011 Programme closure	Tolerance	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
• Longer term capability key (inc. digital capability)-New strategic workforce planning team now in place
• Legacy Portfolio -Capability and maturity mapping exercise to scope the size and scale of the work required

Planned Actions: **Risk to be reviewed 21st November 2024**
No update October 2024
20/09/24
-Working with architecture to define and design the support model for CDO (first, second and third line of support)- ties in to ownership and processes- DEADLINE 3rd October.
-Discussion starting around SPM- fits around ownership- this will require some individual attention due to size (w/c 23rd September 2024).
- Transition- further work to understand and categorise (deep dive) on transition areas. Problem is that the shapes of the organisation make it difficult to transition to agency- looking at the taxonomy of the business structures. Decison made on the future model to be announced October 2024.

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

CR-012 Management information and performance (data)	Tolerance	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.
• Analysis and Insight team produce daily and monthly reports to key operational and executive stakeholders to enable performance management. A number of mitigating controls are in force which include the manual checking, quality assurance and estimates for data points that are not available in SPM. (Some aspect is preventative).
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. The Data Management Checklist embeds data management controls into the release management processes. This ensures relevant data standards are adhered to and grants "Data Management Assurance"(risk-based position ahead of go-live). Documentation can therefore be updated to maintain alignment with data and improve accuracy (new control November 2024).

Preventative

• Working group established that is focused on the medium to longer term resolution of data quality

Planned Actions: **Risk to be reviewed 14th November 2024.**

17/10/24
- Front door requests (improvements) raised into CDO and being evaluated
- Main Realease taking place 18/10/2024 - 20/10/2024
19/09/24
- Business Priority- Data, MI and Analysis Improvement- Scope of initiative to begin 23/09/24.
- In train- project spec being developed for the R:Drive replacement; require a secure and accessible space to hold data without there being "second hand" handlers to provide the data;
- Worry system won't be able to deliver the same information; the system is designed to do so, but testing required.
- Front door request being set up October 2024

Target Score	Target Score Date	Gap To Target	Control Confidence	Risk Appetite	4T's
16	April 2025	4	Limited	Low	Treat
Risk Owner		Ally MacPhail and Andy McClintock	Action Owner	Redacted]	

CR-013 Protective Security	Tolerance	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:

Corrective

• Online security training will be evolved to meet the needs of the Agency to ensure that staff are as aware as they are of data protection and health and safety through a clear programme of instruction and learning

• NPSA Guidance exists and has been drawn upon to address the recent incidents involving the Social Media Auditor, however, the lack of SSS Policy is a vulnerability which is being addressed and policy and directives are in the process of being drafted. This work will be done in coordination with Core SG (SBC) to ensure consistency. In addition, procedures are being introduced for staff to follow when it comes to issues that are either security or relate to security

•Assessment and improvement of security procedures and implementation of corrective measures will follow as a consequence of the CARA work described above

Detective

• CCTV, Guard Force, Security Alarm System are in operation

Directive

• Security Signage and education on smart screens has been introduced.

• 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.

• A dedicated security post has been established to enhance corporate security awareness with the aim to introduce new and relevant security awareness training as well as the introduction of mandatory training.

Preventative

• Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems in place.

• Panic Alarms, Security Vetting, Security Advice/Briefing are in place.

• NPSA Guidance exists and has been drawn upon to address the recent incident.

• Insider Threat Working Group continues developing plans and processes to address the insider threat and this is a collaborative work in progress

• Security awareness and culture development will progress once vulnerabilities are defined, and mitigation is introduced

Planned Actions: **Risk to be reviewed 19th November 2024**

No update September/October 2024-

16/08/24

- Review of procedures for contractor clearance verification and pass issue nearing completion.
- Face to face briefings for mailroom colleagues on specific security threats are ongoing.
- Development of mailroom security procedures to be commenced in September 2024

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

CR-014 Data Protection	Tolerance	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: **Risk to be updated 21st November 2024.**

No update October 2024-

16/09/24:

-Retention and Deletion: A solution design was approved by the Social Security Scotland Architecture Review Board in Aug ’24. A delivery plan is being developed by a joint Social Security Scotland and Social Security Programme team, with an initial release comprised of SPM, Document Management and the Core Enterprise Deletion functionality targeted for mid-2025. CSD has provided resources to assist with discovery work.

19/08/24:

- Annual assurance report was completed and will be considered in September. Complete - Information Governance Group.
- Change Council considered case for change for remote shared drives (unsupported at the end of next year) - what replaces those? Change Council supported the case for change and agreed resources, but challenge is that the organisation cannot currently prioritise this.
- Receipt of distressing personal data on Agency portal will be considered by Change Council in September. New Business Owners have picked up this issue.
- Recently reviewed and signed off the Memorandum of Understanding with the Data Protection Officer.

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

CR-015 Mailroom	Tolerance	25

Social Security Scotland requires a resilient mailroom that delivers a quality service to the organisation, our clients and stakeholders in an efficient and cost-effective way. Without an effective mailroom service and infrastructure, the organisation will fail to meet statutory obligations and published commitments. This will disadvantage clients in digital poverty and negatively impact clients with accessibility issues due to language barriers and disabilities. This will lead to delays in client communications, payments and reputational damage with the public and stakeholders (**rephrased 29/10/24**)

Current Controls:

Corrective

• Policy-Finance: B1 Mailroom Manager works with Finance Business Manager to monitor and control mailroom spend
• IT-- Mailroom work closely with CDO Application Support team to manage system issues
• Resource-- User research work complete and resourcing levels meet current work expectation

Preventative

• IT--Improved productivity (new scanner contract in place May 2024 to 2028)
• Resource-- User research work complete and resourcing levels meet current work expectation
• Resource- Developing Inbound mail & X-ray scanning process- This has now been agreed, Place Services will own the equipment in both Dundee and Glasgow with support from Health & Safety to ensure the equipment is maintained and colleagues are trained appropriately.

Planned Actions: **Risk to be reviewed 6th November 2024.**

04/10/24-

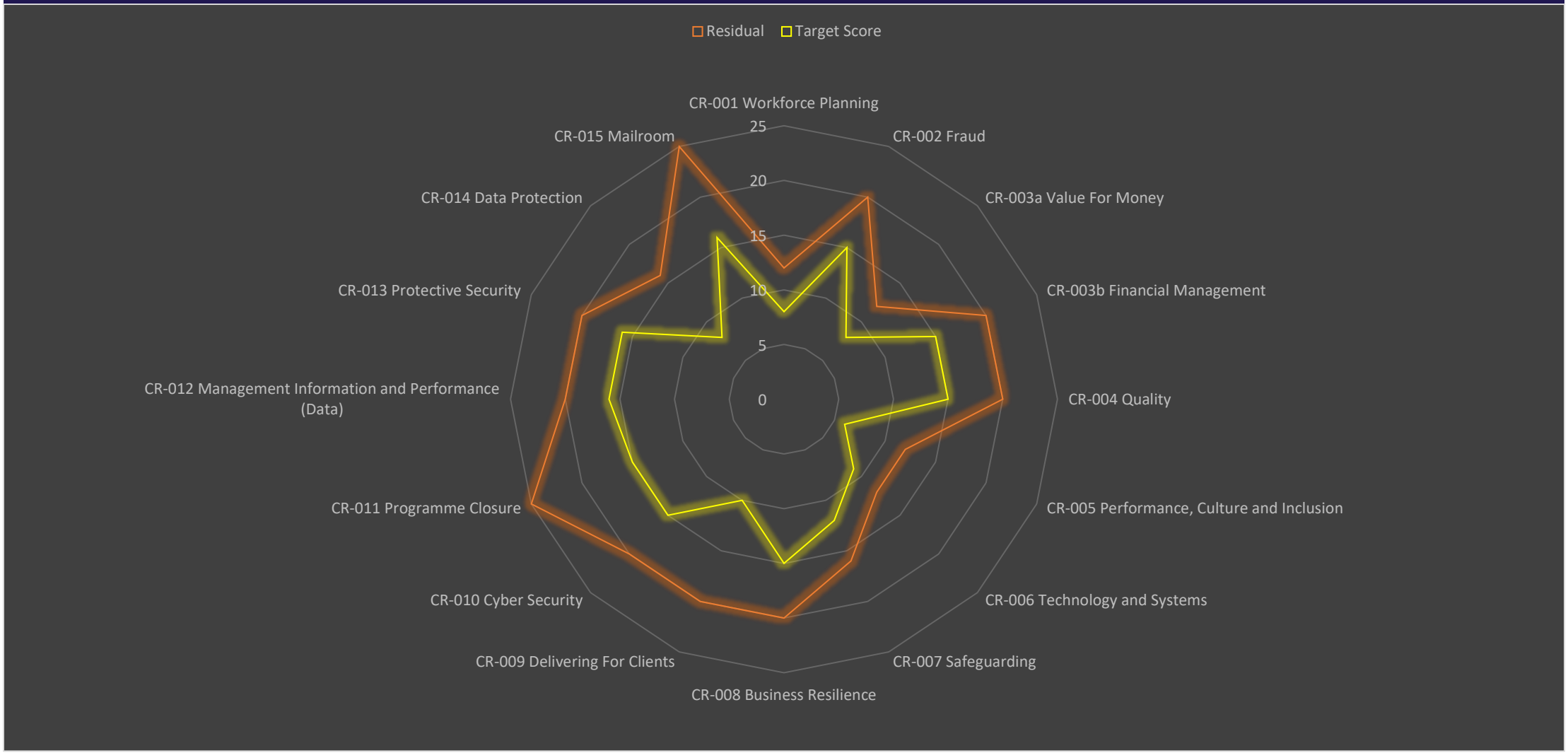
-End of discovery reported to Executive in September- SRO to be approached for decisions, but overall agreements was given with some improvements requiring improvement from Cabinet Secretary (where client journey is impacted).
- SRO report being prepared for presenting to Cabinet Secretary end of October.
- Mono-printing being considered and would have substantial savings (branding may be impacted), but this has been approved and will provide cost saving- awaiting final approval.
- Ownership of mailroom- HR business partner still working through this (roles, responsibilities and position in overall structure)- expected November 2024.
- Review stock ordering process and budget holder responsibilities- work started with Business Analyst support. Next meeting 9th October- now looking at the "to-be" processes using the "as-is" maps to support this and make improvements.
- Top five initiatives for processing will be completed by December 2024- discovery pieces on the remaining six will then begin and the resource will be requested to stay in place (refer to additional information tab for details of initiatives).
- Develop Internal and external communications strategies- Key points for the Saltire page have been drawn out and we will require support from the wider Mailroom team to complete this- Saltire page has now been drafted and is with internal communication team for review.
- Learning routeway- Organisational Development are confident this will be ready by July 2025.

02/09/24

- Contractor mobilised targeting end of calendar year (2024) for completion.
- Mapping and creating guidance to streamline mailroom processes and identify possible efficiencies- The Business Analysts are now in place and assigned to Mailroom until end of this year (December 2024) and will work on this in priority order.
- The BAs are now in place and assigned to Mailroom until end of this year and will work on this in priority order- Learning routeway will not be delivered until 2025 due to resource issues within Organisational Development. However, discussions are ongoing with Health & Safety and Protective Security regarding gaps in processes to keep this moving.
- Nonmatching work queue management and reducing tactical solutions & manual work arounds: Develop Internal and external communications strategies-This is still under discussion as Disability teams have refused to unsubscribe to this Work Queue in the interim
- Working with HRBP to identify resource requirements and recommendations of where mailroom ownership should sit within Agency- Discovery has started and should complete by end of September 2024
- Review stock ordering process and budget holder responsibilities- work started with Business Analyst support. Process maps have been designed and will be discussed with BAs at next stage workshop on 02/09/2024
- Develop Internal and external communications strategies- Key points for the Saltire page have been drawn out and we will require support from the wider Mailroom team to complete this. It is hoped to have this designed and shared with Comms beginning of October 2024
• Explore cost savings including- stock confidence should provide control:- All of these sit with Heather McLaren as part of the notification aspect of these business initiatives. Work is ongoing but impacted by awaiting samples, quotes etc by our Royal Mail and print partner CFH- no confirmed date yet.
• Doc Man Business Owner to spend time with B1 manager before they leave. This action is complete, workshop took place 28/08.
Training suite 4 identified as temporary location and due to be handed over 2nd September.
• Outputs from the Mailroom Discovery work is being presented to Executive Team under Delivery Mode on 3rd October (Key date and require update post meeting). Project expected to last 12-18 months.

Target Score	Target Score Date	Gap To Target	Control Confidence	Risk Appetite	4T's
16	March 2025	9	Insufficient	Low	Treat

Overall Social Security Scotland Risk Profile



Social Security Scotland
Tèarainteachd Shòisealta Alba

Risk Management Team

risk@socialsecurity.gov.scot