




Social Security  
Scotland – Audit and  
Assurance  
Committee- Risk  
Update - February  
2023













**Dignity, fairness, respect.**



## Instructions for using these slides

- Each risk has a CR ref that links to the relevant single page of risk (if not viewing in present mode hold CTRL on the keyboard and left click).
- Each single page of risk has a  Icon to return to the dashboard (if not viewing in present mode hold CTRL on the keyboard and left click).
- Slide 3 shows business plan risk themes and their potential relationship with the strategic risks.

Risk ID	Business Plan Risk Description	Linked Strategic Risks													
BPR-01	Business Plan Risk Theme (1) Having the capacity, capability, resource and organisational resilience to sustain delivery from the Scottish Government Social Security Programme’s complex programme of benefit rollouts to clients that meets our statutory obligations and the values of Our Charter	CR-001	CR-002	CR-004	CR-005	CR-006	CR-007	CR-008	CR-009	CR-010	CR-011	CR-013			
BPR-02	Business Plan Risk Theme (2) Working with the Scottish Government’s Social Security Programme on maturing and developing the performance of our systems and processes to manage an increasing caseload, including improving management and performance information and our fraud and error controls	CR-002	CR-004	CR-006	CR-007	CR-010	CR-011	CR-012	CR-014						
BPR-03	Business Plan Risk Theme (3) Working with the Scottish Government’s Social Security Programme on managing key relationships and dependencies to ensure that digital services meet clients’ needs and we minimise the impact of technical debt and impacts to our change management function	CR-002	CR-007	CR-008	CR-009	CR-011	CR-014								
BPR-04	Business Plan Risk Theme (4) Dealing with economic uncertainty and the impact on forecasting future benefit expenditure and the consequent impact on our administrative budgets and workforce planning	CR-003a	CR-003b	CR-007	CR-008	CR-012									

Risk ID	Risk Description (One line description)	Inherent Risk Score	Residual Risk Score	Score Change (Since last reporting)	Target Risk Score	4 T's	Risk Owner	Action Owner(s)
<a href="#">CR-001</a>	Workforce planning and organisational design	20	12		6	Treat	Nicola Rudnicki	
<a href="#">CR-002</a>	Fraud	25	20		15	Treat	James Wallace	
<a href="#">CR-003a</a>	Value for Money	20	12		9	Treat	James Wallace	
<a href="#">CR-003b</a>	Financial Management	20	20		15	Treat	James Wallace	
<a href="#">CR-004</a>	Quality	25	20		15	Treat	Gayle Devlin and Janet Richardson	
<a href="#">CR-005</a>	Performance, Culture and Inclusion	9	12		6	Treat	Ally MacPhail and Nicola Rudnicki	
<a href="#">CR-006</a>	Technology and systems	16	12		9	Treat	Andy McClintock	
<a href="#">CR-007</a>	Safeguarding	20	16		12	Treat	Gayle Devlin and Janet Richardson	
<a href="#">CR-008</a>	Organisational resilience	25	16		12	Treat	Ally MacPhail	
<a href="#">CR-009</a>	Delivering for our clients	25	20		10	Treat	Ally MacPhail and Janet Richardson	
<a href="#">CR-010</a>	Cyber security	25	15		10	Treat	Andy McClintock	
<a href="#">CR-011</a>	Programme closure	25	25		15	Treat	Ally MacPhail	
<a href="#">CR-012</a>	Management Information and Performance (Data)	20	20		16	Tolerate	Ally MacPhail and Andy McClintock	
<a href="#">CR-013</a>	Protective Security						Nicola Rudnicki	
<a href="#">CR-014</a>	Data Protection						Janet Richardson, Professor Paul Knight and Andy McClintock	



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.

Inherent Impact Score	Inherent Likelihood Score
4	5

Inherent Risk Score
20

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Budget approach agreed with Workforce Planning 24/25- lessons learned are being used from previous years.
- HR Business Partners will be more involved with Deputy Directors (both support and challenge) to ensure decision are based on priorities.
- Recruitment controls and exceptions process- all roles within the organisation go through governance and approvals prior to any recruitment; this is with consideration to affordability as well as role requirement.
- Establishing Control Document (ECD)- Governing document that ensures people take responsibility for their own area to understand headcount enabling finance to predict what our future forecasts look like.
- Re-structuring and re-deployment guidance and policy aligned with Scottish Government.

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- Finance to investigate workforce design principles and the work on the budget approach
- Second phase of ERP (Enterprise Resource Planning systems for HR) that will allow future planning and resourcing- workforce planning tool - April 2024 - 15/01/24: ERP has been delayed

Residual Impact Score	Residual Likelihood Score
4	3

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
Increase from 9 to 12	Nicola Rudnicki		6	Treat

Residual Risk Score

12
----





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.

Inherent Impact Score				Inherent Likelihood Score	
5				5	
Inherent Risk Score					
25					
Mitigating Controls					
<p><i>Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)</i></p> <p><b>Preventative:</b></p> <ul style="list-style-type: none"> <li>• Fraud Awareness sessions are a mandatory part of induction learning.</li> <li>• 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 &amp; 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.</li> <li>• 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.</li> <li>• Fraud Champion network which empowers Operational colleagues to support each other and provides a “direct line” to the Risk Analysis and Control team.</li> <li>• BPSS check (or higher level of National Security Vetting depending on role) for all new colleagues joining the organisation.</li> </ul>			<p><b>Corrective:</b></p> <ul style="list-style-type: none"> <li>• Counter fraud function in place, with appropriately trained specialist colleagues.</li> </ul> <p><b>Detective:</b></p> <ul style="list-style-type: none"> <li>• Cyber defence in place, live monitoring.</li> <li>• Counter fraud function in place, with appropriately trained specialist colleagues.</li> <li>• Public fraud reporting line in place and open.</li> </ul>		
Planned Actions					
<p><i>Dates to achieve Target Risk Score</i></p> <p><i>Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).</i></p> <p><b>Preventative:</b></p> <ul style="list-style-type: none"> <li>• Improvements to digital capability requested from Social Security Programme</li> <li>• First line control improvements to be requested from Client Services Delivery</li> <li>• Deep Dive Risk Assessments into “as is” benefit delivery and processes will enable identification of fraud and error vulnerabilities therein.</li> <li>• Sample Work of specific benefit criteria will continue, allowing quantification and measurement of assumed risks and threats. Improvement can then be better framed.</li> <li>• Work to be taken forward to continue to build culture of fraud awareness and responsibility for prevention across the organisation.</li> </ul>			<p><b>Detective:</b></p> <ul style="list-style-type: none"> <li>• Improvements to digital capability requested from Social Security Programme.</li> <li>• First line control improvements to be requested from Client Services Delivery.</li> <li>• Technology roadmap for fraud management and data layer being developed.</li> <li>• Policy/Legal changes to facilitate measurement.</li> </ul> <p><b>Corrective:</b></p> <ul style="list-style-type: none"> <li>• Improvements to digital capability requested from Social Security Programme</li> <li>• First line control improvements to be requested from Client Services Delivery</li> </ul>		
Residual Impact Score				Residual Likelihood Score	
5				4	
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's	
Added to register February 2024	James Wallace		15	Treat	
Residual Risk Score					
20					



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.

## Inherent Impact Score

4

## Inherent Likelihood Score

5

## Inherent Risk Score

20

## Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Well-developed corporate governance including Executive Advisory Board, Audit and Assurance Committee, Regular ET meetings, Portfolio Sponsor meetings and the Finance and Investment Forum.
- Presence of non-execs on our board. Scrutiny from Scottish Government and Parliament.
- Range of assurance work from Internal and External Audit (Audit Scotland).
- Agency Framework document up to date and reviewed regularly; scheme of delegated budgets in place.
- Regular monitoring and reporting of financial position.
- Investment in finance business partnering and support to business areas from Finance on internal control and value for money.
- Arrangement for Corporate and Business Planning are in place and linked to budgets. Reporting through our Annual Report linked to performance and expenditure.

## Planned actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- On-going discussions around arrangements for capturing what we do on our savings programme and full update once this work is completed and tied to the budget- Due late February 2024

## Residual Impact Score

3

## Residual Likelihood Score

4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	James Wallace		9	Treat

## Residual Risk Score

12



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.

Inherent Impact Score	Inherent Likelihood Score
4	5

Inherent Risk Score
20

#### Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Regular monitoring and reporting of in-year financial position (monthly basis)
- Financial Planning Function in place with a mid-term financial plan prepared and regularly updated (quarterly basis)
- Close working between Finance and Workforce Planning colleagues and analysts- workforce plans and staffing requirements (monthly basis)
- Finance Business Partner arrangements in place for the organisation.
- Benefit forecasting review group in place which considers demand for benefits and spend and forecast full year position (monthly meeting)
- 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).
- Prompt business planning/prioritisations- work with Governance plan on priorities and business change- Small working group- (Fortnightly).

#### Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- Finance and Investment forum- sharing medium term plans- (meets monthly)- part of overall governance providing assurance more than delivering on actions; assurance provided from visibility of medium-term plans and being able to challenge. The forum will consider future financial implications with a required business case required for in-year and future year changes; forum maturing before becoming control/mitigation.
- Workshops will finish in January with a view to informing overall finances available to Agency and Programme.
- Budget negotiations- settlement known (early December 2023). From SG- we now have our 24-25 budget settlement, and the work continues to set a balanced budget based on priorities by end March 24.
- Transition work. Workshops happening late Nov/early Dec with a better view available Jan 2024.

Residual Impact Score	Residual Likelihood Score
5	4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	James Wallace		15 ↑	Treat

#### Residual Risk Score

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.

Inherent Impact Score	Inherent Likelihood Score
5	5

Inherent Risk Score
25
Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- 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 (corrective).
- Functionality on unapplied deductions for payment correction cases- NB -Incorrect processing of payment correction cases are one of the largest error areas in Low Income Benefit. 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 (corrective).
- 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) (preventative)
- 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 (preventative/corrective).
- Error Control Strategy for the Agency is in place- being refreshed and awaiting publication (directive)
- Checks- 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) (preventative).
- Organisational Improvement Team discuss the errors monthly- continuous improvement approach applied to triage any improvement required (detective).

**Planned Actions**

*Dates to achieve Target Risk Score*  
*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- Error Control Working Group (Monetary Value of Fraud and Error meeting)- group agreed thirteen recommendations- looking at understanding the gaps between checking operational processes and what is in place in Fraud Error Resolution Unit.
- Power BI being used to capture colleague feedback and analysis will be used to produce more in-depth reporting (checking quality); Power BI roll out underway and complete by Dec 2023
- Internal Audit review on internal controls that is out for approval from management- Final report under discussion (Feb 2024)
- One of the thirteen recommendations- working with analysts to bring error modelling under control- in and out flow of error- End of February 2024.
- Deloitte report on official error in CDP to be added; once reports are signed off this will be rolled up with the thirteen recommendations from the Error Control Working Group; Quality plan may be put in place to drive that forward- Mid January 2024

Residual Impact Score	Residual Likelihood Score
5	4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	Janet Richardson and Gayle Devlin		15	Treat

Residual Risk Score
20



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.

## Inherent Impact Score

3

## Inherent Likelihood Score

3

## Inherent Risk Score

9

## Mitigating Controls

Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)

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

## Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- More testing for ERP system as there is a delay.
- Diversity & Inclusion strategy under review- Summer 2024
- Linking up the work of the Accessibility team with the broader work of People Services to ensure it is sustainable in the long-term April 2024.

## Residual Impact Score

3

## Residual Likelihood Score

4

Score Change (since last reporting)

Risk Owner

Action Owner(s)

Target Risk Score

4T's

Increase from 6 to 12

Ally MacPhail and Nicola Rudnicki

6

Treat

## Residual Risk Score

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.

Inherent Impact Score	Inherent Likelihood Score
4	4

16
----

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Tracking of technical debt (size and estimated value) (Detective)
- Tracking the life cycle of technology applications with a view to future upgrades and/or replacement.(Preventative)
- Live service monitoring and service management, including the ability to record and track faults, defects and system availability (help desk). (Detective)
- Back up and disaster recovery arrangements in place. (Corrective)
- Significant digital competence and capability. (Corrective)

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

Residual Impact Score	Residual Likelihood Score
4	3

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	Andy McClintock		9	Treat

Residual Risk Score

12
----



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.

Inherent Impact Score	Inherent Likelihood Score
4	5

Inherent Risk Score
20

#### Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Social Security Scotland has set up a group of health and social care staff that which consists of registered professionals, including social workers who have previous experience in handling cases which involves child and adult protection. (Directive)
- 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. (Corrective)
- 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. (Directive)
- Dedicated team in place managing safeguarding of professionals (qualified team) (Preventative)
- Quality Support Team within Client Services Delivery- checking the standard of claims made and independent checks of 'post events' including checking if safeguarding has been applied or was appropriate. (Detective)

#### Planned Actions

Dates to achieve Target Risk Score

Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).

- 

Residual Impact Score	Residual Likelihood Score
4	4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	Janet Richardson and Gayle Devlin		12	Treat

#### Residual Risk Score

16
----



Social Security Scotland must be resilient in the face of any major development, event or crisis. The systems and processes supporting our core operations must be maintained, enhanced and continuously improved to ensure they are as resilient to disruption as possible, or can be quickly and effectively recovered, to minimise impact on clients and staff.

Inherent Impact Score	Inherent Likelihood Score
5	5

Inherent Risk Score
25

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Major Incident and Business Continuity Frameworks provide the backbone of business resilience. They provide the required information on how disruptive events are managed across the organisation, and what the agreed incident response structures and escalation routes are. (Directive)
- The business resilience team provides the necessary training and upskilling to business continuity teams, to allow for the development of their respective branch/team business continuity plans. Plans are then reviewed and exercised biannually to validate contents and to ensure business continuity teams are confident in responding to a series of disruptive events using these plans. (Preventative)
- Post incident debriefs are conducted following each incident, to learn from lessons identified and to continuously improve how we respond and recover to incidents (Detective)
- Executive Team have been included in several upskilling and exercising session, to ensure there is top management commitment to resilience. (Detective)

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

- Session was held in December with Executive Team to discuss business continuity priorities. A list has been shared, with Executive Team to provide further comments by end of January 2024.
- Further discussions have taken place with external stakeholders in relation to horizon scanning. The Business Resilience Team now have access to wider government publications that provide information on the threat landscape , in particular to government organisations.

Residual Impact Score	Residual Likelihood Score
4	4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	Ally MacPhail		12	Treat

Residual Risk Score

16
----



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.

Inherent Impact Score

5

Inherent Likelihood Score

5

Inherent Risk Score

25

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

Risk Controls to be split to the following and updated in the next reporting cycle::

- Assurance for Business as Usual
- Continuous improvement activities are on-going to improve our work, to continue to sustain processes
- Measurements of performance (Performance Pack)- what does this tell us?
- Internal Audit reports.
- Single prioritised backlog.

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

Residual Impact Score

5

Residual Likelihood Score

4

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
Increase from 10 to 20	Janet Richardson and Ally MacPhail		10	Treat

Residual Risk Score

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.

Inherent Impact Score	Inherent Likelihood Score
5	5

Inherent Risk Score
25

**Mitigating Controls**  
*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Technical protective security controls are applied to the digital estate in line with industry best practice and cyber security frameworks. (Preventative).
- 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. (Directive).
- Vulnerability management processes enable vulnerabilities to be identified and remediated on a scheduled basis.
- Threat intelligence tools are used to identify new or emerging threats and to inform the selection and configuration of protective controls and activities. (Preventative).
- 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. (Preventative).
- Security assurance assessments are also undertaken, where relevant, as part of standard procurement processes. (Directive).
- Standardised risk management processes are conducted to define the security risks associated with new systems, initiatives, services, and procurements. (Directive).
- Event logging, monitoring, alerting, and investigating is continually undertaken to identify and resolve any suspicious activity related to cyber security (Directive).
- Regular collaboration occurs with the UK's National Cyber Security Centre (NCSC) and the Scottish Government's Cyber Resilience Unit.
- Incident response plans are defined and regularly exercised. (Directive).
- Monitoring of Systems and system activities. (Directive).
- Technical environments monitored by a range of tools and software services. (Directive).

**Planned Actions**

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

Residual Impact Score	Residual Likelihood Score
5	3

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No Change	Andy McClintock		10	Treat

Residual Risk Score
15



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 and capacity to run, maintain and change those services.

## Inherent Impact Score

5

## Inherent Likelihood Score

5

## Inherent Risk Score

25

## Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

- Key areas of control:
- Longer term capability key (inc. digital capability)
    - Exceptions process includes requirement to liaise with relevant support team members who will help to identify where a role could be filled through internal moves within that area. (Preventative)- from divisional risk PPR-02
    - Business Planning work commenced to better understand business critical activities which will assist in prioritisation of roles and work (Preventative)- from divisional risk PPR-02
  - Operating Model- service structure
  - Change Structures
  - Legacy Portfolio

## Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

The key areas of control will determine the action owners- currently being assigned and discussion to take place Feb 2024.

- Single Prioritised Backlog work continues
- Work in finance area to understand what we need to undertake improvements.
- Agency to look at structures to be fully accountable for improving our services.

## Residual Impact Score

5

## Residual Likelihood Score

5

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
No change	Ally MacPhail	New action owners to be assigned	15	Treat

## Residual Risk Score

25



Social Security Scotland must generate good quality management information and performance data 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.

Inherent Impact Score		Inherent Likelihood Score	
5		4	

Inherent Risk Score			
20			

**Mitigating Controls**  
*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*  
 Discussion with Risk Owners 15/01/24

**Planned Actions**  
*Dates to achieve Target Risk Score*  
*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*  
 Discussion with Risk Owners 15/01/24  
 - More MI deliverables in 2024 - release schedule will provide detail  
 - Data strategy goes beyond MI and is critical to this risk

Residual Impact Score		Residual Likelihood Score	
5		4	

Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	4T's
	Ally MacPhail and Andy McClintock	New action owners to be assigned	16	

Residual Risk Score			
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.

Inherent Impact Score

Inherent Likelihood Score

Inherent Risk Score

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

*Accepted to Corporate Risk Register 25/01/24- initial assessment to be conducted 14/02/24*

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

Residual Impact Score

Residual Likelihood Score

Score Change (since last reporting)

Risk Owner

Action Owner(s)

Target Risk Score

4T's

Nicola Rudnicki

New action owners to be assigned

Residual Risk Score



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 would result in unauthorised access, sharing or loss of personal data leading to poor client service, increased costs, inefficiencies, compensation, reputational damage and regulatory enforcement action

Inherent Impact Score

Inherent Likelihood Score

Inherent Risk Score

Mitigating Controls

*Current controls that are managing the risk (type of control and details of mitigating nature of control- e.g. how, what, who?)*

*Accepted to Corporate Risk Register 25/01/24- awaiting date for initial assessment.*

Planned Actions

*Dates to achieve Target Risk Score*

*Named Action Owners if different from below (e.g. an action may be progressed by Programme, Project Management Office or other business Area).*

Residual Impact Score

Residual Likelihood Score

Score Change (since last reporting)

Risk Owner

Action Owner(s)

Target Risk Score

4T's

Janet Richardson,  
Professor Paul Knight and  
Andy McClintock

New action owners to be  
assigned

Residual Risk Score

