







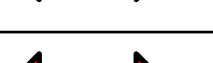










Social Security
Scotland – Audit and
Assurance
Committee- Risk
Update – May 2024

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	Risk Description (One line description)	Inherent Risk Score	Residual Risk Score	Score Change (Since last reporting)	Target Risk Score	Target Score Date	4 T's	Risk Owner	Action Owner(s)
CR-001	Workforce planning and organisational design	20	12		8	March 2025	Treat	Nicola Rudnicki	[Redacted]
CR-002	Fraud	25	20		15	April 2029	Treat	To be assigned	[Redacted]
CR-003a	Value for Money	20	12		9	March 2025	Treat	To be assigned	[Redacted]
CR-003b	Financial Management	25	20		15	April 2025	Treat	To be assigned	[Redacted]
CR-004	Quality	25	20		15	March 2025	Treat	Gayle Devlin and Janet Richardson	[Redacted]
CR-005	Performance, Culture and Inclusion	9	12		6		Treat	Ally MacPhail and Nicola Rudnicki	[Redacted]
CR-006	Technology and systems	16	12		9	December 2024	Treat	Andy McClintock	[Redacted]
CR-007	Safeguarding	20	16		12	August 2025	Treat	Gayle Devlin and Janet Richardson	[Redacted]
CR-008	Organisational resilience- Risk under review								[Redacted]
CR-009	Delivering for our clients	25	20		10	December 2025	Treat	Ally MacPhail and Janet Richardson	[Redacted]
CR-010	Cyber security	25	20		10		Treat	Andy McClintock	[Redacted]
CR-011	Programme closure	25	25		15	April 2025	Treat	Ally MacPhail	[Redacted]
CR-012	Management Information and Performance (Data)	20	20		16		Tolerate	Ally MacPhail and Andy McClintock	To be assigned
CR-013	Protective Security	25	20		16	April 2025	Treat	Nicola Rudnicki	[Redacted]
CR-014	Data Protection	20	16		8		Treat	Janet Richardson, Professor Paul Knight and Andy McClintock	To be assigned

CR-002 Fraud				Reporting Period- 04-24	
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					
<ul style="list-style-type: none">• Preventative:• 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.• 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.					
Planned Actions					
20/03/24: -[Redacted] Preventative: <ul style="list-style-type: none">• Improvements to digital capability requested from Social Security Programme• First line control improvements to be requested from Client Services Delivery• Deep Dive Risk Assessments into “as is” benefit delivery and processes will enable identification of fraud and error vulnerabilities therein.• Sample Work of specific benefit criteria will continue, allowing quantification and measurement of assumed risks and threats. Improvement can then be better framed.• Work to be taken forward to continue to build culture of fraud awareness and responsibility for prevention across the			Detective: <ul style="list-style-type: none">• Improvements to digital capability requested from Social Security Programme.• First line control improvements to be requested from Client Services Delivery.• Technology roadmap for fraud management and data layer being developed.• Policy/Legal changes to facilitate measurement. Corrective: <ul style="list-style-type: none">• Improvements to digital capability requested from Social Security Programme• First line control improvements to be requested from Client Services Delivery		
Residual Impact Score			Residual Likelihood Score		
5			4		
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Scored Date	4T's
Added to register February 2024	James Wallace	[Redacted]	15	April 2029	Treat
Residual Risk Score					
20					

CR-003a- Value for Money				Reporting Period- 04-24	
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				Inherent Likelihood Score	
4				5	
Inherent Risk Score					
20					
Mitigating Controls					
<div>Controls Headings:</div> <div><div><div>• Economy- raw measure of cost</div><div>• Efficiency- how quickly we do it</div><div>• Effectiveness- Outcome- what is the impact of what we are doing</div></div><div><div>• Performance Forum- collective leadership that assesses performance risk and issues; including value for money. This then provides updates Executive Team; fortnightly (Corrective).</div><div>• Savings that have been identified within areas agreed by Executive Team will be project managed; Finance track progress through the Finance and Investment Forum (Corrective)- Efficiency and Effectiveness</div></div></div>					
Planned actions					
<div>Discussion with Action Owner(s) 23/04/24:</div> <div><div>• Governance arrangements around projects identified and in flight.</div><div>• Taking action to discuss what might be best arrangements to support savings- workshop arranged to look at this.</div><div>• Staffing principles being reviewed- consideration of sustainable longer-term model/</div><div>• Future needs being reviewed, specifically workforce.</div></div>					
Residual Impact Score				Residual Likelihood Score	
4				3	
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
No Change	James Wallace	[Redacted]	8	March 2025	Treat
Residual Risk Score					
12					

CR-003b- Financial Management				Reporting Period- 04-24	
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	
5				5	
Inherent Risk Score					
25					
Mitigating Controls					
Key Controls					
<ul style="list-style-type: none">Regular monitoring and reporting of in-year financial position (monthly basis) (Detective)Financial Planning Function in place with a mid-term financial plan prepared and regularly updated (quarterly basis) (Directive)Close working between Finance and Workforce Planning colleagues and analysts- workforce plans and staffing requirements (monthly basis) (Preventative)Finance Business Partner arrangements in place for the organisation.(Preventative)Benefit forecasting review group in place which considers demand for benefits and spend and forecast full year position (monthly meeting) (Preventative)Director General Finance Forum (Fortnightly meeting) (Preventative)Close working with Scottish Government Finance colleagues on arrangement for resource spending reviews (annual cycle as linked to budget). (Preventative)Prompt business planning/prioritisations- work with Governance plan on priorities and business change- Small working group- (Fortnightly). (Preventative)					
Planned Actions					
15/04/24					
<ul style="list-style-type: none">Executive Team have agreed divisional level budget allocations in line with our business planning priorities. This does not change the score at present. There won't be any change for the next two months (financial reporting unavailable until first quarter).					
Inherent score increased to 25 from 20 (increase of impact from 4 to 5)					
Residual Impact Score				Residual Likelihood Score	
5				4	
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
No Change	James Wallace	[Redacted]	15	April 2025	Treat
Residual Risk Score					
20					

CR-004- Quality				Reporting Period- 04-24	
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					
Controls					
<ul style="list-style-type: none">• 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)• Current checks providing control :• 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) 30/04/24- Four new members joined Quality and Performance team improving checks for full end to end journey(preventative).• Organisational Improvement Team discuss the errors monthly- continuous improvement approach applied to triage any improvement required (detective).					
Planned Actions					
30/04/24					
<ul style="list-style-type: none">• Quality framework (draft v1.0) completed; meeting with Deloitte who will provide feedback then out to stakeholders for Quality Review (error control group and internal controls team);• Disability Intervention service now receiving live referrals from operations (CSD); data will be provided each month/quarter (update June 2024 for Q1 report).• [Redacted]					
20/03/24					
<ul style="list-style-type: none">• MS forms use has been approved. Tools now in place to feedback data on quality- removal of CSD-OR022. Divisionally this will work (CSD) but for broader strategic level this is a good start. Power BI will come in to play on feedback (once Power BI available).• how do we ensure that product leads are able to respond to large errors within the timescales. WE have better insight, but do we have the capacity to make improvements to skills and processes possibly remains a concer.• Scrum team has been allocated to do discovery work on causes of payment correction cases to see how volume of value can be reduced. Release time in October release to make system changes (hoping) and guidance changes; operational structure may also change to improve efficiency (October 2024)- this is an overall agency efficiency improvement (value for money impact).• Opening disability intervention queues for reactive work (1st April 2024)- non-medical changes- once issues and volumes understood that may expand beyond non-medical changes.• Deep dive into errors- will this provide any additional insight for product owners etc; starting with Scottish Child Payment. (May 2024).					
Residual Impact Score			Residual Likelihood Score		
5			4		
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
No Change	Janet Richardson and Gayle Devlin	[Redacted]	15	March 2025	Treat
Residual Risk Score					
20					

Inherent Impact Score					Inherent Likelihood Score				
4					4				
16									
Mitigating Controls									
31/01/24- Update (GM) • [Redacted]									
Planned Actions									
23/04/24 • Maturity Assessment of Digital services to inform medium to long term planning for retirement or refresh of the Digital estate; CDO will sponsor an independent assessment of our core Digital services to assess current & future alignment to business and service needs. As part of this process we will identify any Digital services that is approaching retirement or end of life. The output of this assessment will inform our medium to long term plan for future Digital investment									
Residual Impact Score					Residual Likelihood Score				
4					3				
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's				
No Change	Andy McClintock	[Redacted]	9	December 2024	Treat				
Residual Risk Score									
12									

CR-007- Safeguarding				Reporting Period- 04-24	
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					
Controls					
<ul style="list-style-type: none">• Social Security Scotland has set up a group of health and social care staff that includes 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- 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. (Detective)• 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 (Detective)• Implementation of regulations (16th January) increased responsibility to organisation- defined legislative responsibility in safeguarding (Directive).					
Planned Actions					
16/04/24					
<ul style="list-style-type: none">• [Redacted]					
Residual Impact Score				Residual Likelihood Score	
4				4	
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
No Change	Janet Richardson and Gayle Devlin	[Redacted]	12	August 2025	Treat
Residual Risk Score					
16					

CR-008- Organisational Resilience					Reporting Period- 01-24	
Risk under review						
Inherent Impact Score				Inherent Likelihood Score		
5				5		
Inherent Risk Score						
25						
Mitigating Controls						
Planned Actions						

CR-009 Delivering for our clients				Reporting Period- 04-24	
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			Inherent Likelihood Score		
5			5		
Inherent Risk Score					
25					
Mitigating Controls					
Controls					
Assurance for Business as Usual					
• •Quality Strategy- post payment checks, and feedback look in place (Corrective)					
Continuous improvement activities are on-going to improve our work, to continue to sustain processes					
• •Quality Strategy- post payment checks, and feedback look in place (Corrective)					
Measurements of performance (Performance Pack)- what does this tell us?					
• •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)					
• Single prioritised backlog.					
Planned Actions					
25/04/24					
• Business Priorities- as identified by Executive Team- we are due to meet ET 21st May to walkthrough the scope of all the initiatives, one of which is the Operational Delivery Improvements. Following this meeting we will have a better idea of the scope, timing and sequence of this work.					
• Continuous Improvements- three-month piece of work to understand what a Continuous Improvements Function for Agency might look like.					
• Performance- HR piece of work that is helping us to discuss performance in a different way. This looks at every aspect of performance at a team level- e.g. how are we doing against a range of activities; this has commenced within CDP, is currently being rolled out in ADP and planned for Client Experience.					
28/03/24					
• Work underway to establish an Agency Data Service- full data service review by end of April 2024- data and MI road map.					
• PI (Priority Improvement) planning in programme prioritising what Agency needs (currently undertaking May PI planning and looking at Single Prioritised Backlog for MI and reporting.					
• Telephony improvement plan- wide ranging project based on the Simpler Workshop- work is all on track (e.g.- understanding why people are calling the agency and rationalising the call completion codes, standardising this across the piece for more reliable data).					
• Work to understand what reviews look like- currently uncertain of numbers and where they are- now trying to quantify this work and generate confidence in the numbers of reviews.					
• Centre of Excellence work underway to increase automation and improving- six areas (test areas)- straight through processing for SI Part 1, or auto rejection of Part 1 forms if incomplete (ADP and CDP).					
• Performance and Productivity- work underway discussing team performance within CDP areas (Leadership and Strategic Capability delivering sessions).					
Residual Impact Score			Residual Likelihood Score		
5			4		
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
Increase from 10 to 20	Janet Richardson and Ally MacPhail	[Redacted]	10	December 2025	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	

19/04/24

- New head of Security Ops now in place (**Preventative**)

21/03/2

- [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**).

06/11/23

- 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 (**Corrective**).
- Threat intelligence tools are used to identify new or emerging threats and to inform the selection and configuration of protective controls and activities (**Detective**).
- 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 (**Preventative**).
- 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 (**Corrective/Preventative**).
- Regular collaboration occurs with the UK's National Cyber Security Centre (NCSC) and the Scottish Government's Cyber Resilience Unit (**Directive**).
- Incident response plans are defined and regularly exercised (**Corrective/Preventative**).


Planned Actions

Update 19/04/24

- [Redacted]

Residual Impact Score				Residual Likelihood Score	
5				4	
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Risk Score Date	4T's
No Change	Andy McClintock	[Redacted]	10		Treat
Residual Risk Score					
20					

CR-011 Programme closure			Reporting Period- 04-24		
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.					
Inherent Impact Score			Inherent Likelihood Score		
5			5		
Inherent Risk Score					
25					
Mitigating Controls					
Controls					
<ul style="list-style-type: none">Longer term capability key (inc. digital capability)<ul style="list-style-type: none">New strategic workforce planning team now in place (Preventative)Operating Model (service structure)Change StructuresLegacy Portfolio<ul style="list-style-type: none">Capability and maturity mapping exercise to scope the size and scale of the work required (Preventative).					
Planned Actions					
16/04/2024					
Long term Capability:					
<ul style="list-style-type: none">Contractors will remain till the end of June 2024 for End-to-End Future Service Initiative.					
Change Structures:					
<ul style="list-style-type: none">Change Delivery Model aimed for end of March 2024 has been completed. Testing is no longer required within this workstream as it will be covered in Continuous Improvement and Portfolio Management Office workstreams.					
19/03/24					
Legacy Portfolio:					
<ul style="list-style-type: none">Completion of level 2 maturity assessment- April 2024Validation of full end to end maturity capability/full business planning- May 2024Business planning to understand the key actions to increase maturity in the priority areas- May 2024Full map of transitions against capability to plan future road map May 2024Legacy Portfolio under review- once capability planning complete this will drive focus on what the portfolio needs to do.					
Residual Impact Score			Residual Likelihood Score		
5			5		
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Risk Score	4T's
No change	Ally MacPhail	[Redacted]	15	April 2025	Treat
Residual Risk Score					
25					

CR-012 Management Information and Performance (Data)				 Reporting Period- 12-23	
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					
Full assessment still to take place- awaiting confirmation from Action Owners.					
Planned Actions					
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					

CR-013 Protective Security			Reporting Period- 04/24		
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		
5			5		
Inherent Risk Score					
25					
Mitigating Controls					
Physical <ul style="list-style-type: none">Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems exist [Redacted](Preventative); CCTV, Guard Force and Security Alarm Systems are in place and act as a detective control as well as a preventative control (Detective); Security signage (Directive)					
Personnel <ul style="list-style-type: none">Panic Alarms, Security Vetting, Security Advice/Briefing are currently in place, [Redacted](Preventative); National Security Vetting Policy which is mandated for all staff requiring a security clearance. [Redacted] (Directive)					
Security Culture <ul style="list-style-type: none">Minimal signage (Directive); [Redacted] (Corrective/Directive)					
Counter Terrorist <ul style="list-style-type: none">Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems (Preventative); CCTV, Guard Force, Security Alarm System (Detective); Security briefings currently contain reference to CT [Redacted] (Corrective)					
Security Policy and Directives <ul style="list-style-type: none">NPSA Guidance exists and is comprehensive. [Redacted] (Preventative and corrective); Introduction of new policy and directives (Directive)					
Insider threat. <ul style="list-style-type: none">Insider Threat Working Group has been formed to address the risk through a collaboration between key Divisions (Preventative); Security awareness and culture being introduced [Redacted] (Preventative).					
Security of Information (non-cyber) <ul style="list-style-type: none">Critical Asset Risk Assessment being commenced which covers information security out with the cyber area (Preventative); Ongoing assessment of existing procedures with a view to implement corrective measures (Corrective)					
Residual Impact Score			Residual Likelihood Score		
5			4		
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Score Date	4T's
	Nicola Rudnicki	[Redacted]	16	April 2025	Treat
Residual Risk Score					
20					

Planned actions captured on next slide



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.

Planned Actions

- Physical**
- Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems are being [Redacted] . More enhancements in guarding procedures and CCTV coverage is on the horizon and will also be driven by the Critical Asset Risk Assessment (**Preventative**)
 - CCTV, Guard Force, Security Alarm System is also a preventative as well as a detective matter which is being addressed as outlined above (**Detective**).
 - Security Signage and education on smart screens has been introduced [Redacted] Work is ongoing with internal communications as well as drawing from NPSA guidance (**Directive**).


- Personnel**
- Whilst Panic Alarms, Security Vetting, Security Advice/Briefing are in place, [Redacted] (**Preventative**).
 - 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. Security Culture (**Directive**)
 - [Redacted] . 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. Enhanced signage throughout buildings and on monitors will also be developed (**Directive**).
 - 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 (**Corrective**).

- Counter Terrorist**
- Secure Doors, Barriers, Speed Gates (control of entry), CCTV, Guard force, Secure Rooms, Security Alarm Systems however, [Redacted] In addition, planned security exercises utilising "table top" exercises in the first instance are being planned in partnership with Police Scotland and, in addition, with the UK Protective Security Centre (**Preventative**).
 - CCTV, Guard Force, Security Alarm System are in operation, but their enhancement is underway to deliver greater defence in depth (**Detective**).

- Security Policy and Directives**
- NPSA Guidance exists and has been drawn upon to address the recent incidents [Redacted] 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 (**Preventative & Corrective**).
 - Introduction of new policy and directives as described above (**Directive**).

- Security of Information (non-cyber)**
- Critical Asset Risk Assessment has commenced in order to identify critical assets, many of which are information assets. [Redacted] (**Preventative**).
 - Assessment and improvement of security procedures and implementation of corrective measures will follow as a consequence of the CARA work described above (**Corrective**).

- Insider threat**
- Insider Threat Working Group continues developing plans and processes to address the insider threat and this is a collaborative work in progress (**Preventative**).
 - Security awareness and culture development will progress once vulnerabilities are defined and mitigation is introduced (**Preventative**).

CR-014 Data Protection						Reporting Period- 04/24	
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.							
Inherent Impact Score				Inherent Likelihood Score			
4				5			
Inherent Risk Score							
20							
Mitigating Controls							
Controls <ul style="list-style-type: none">• e-learning (directive)• Routine communications (directive)• Lessons learned from previous breaches (preventative)• Data retention strategy (preventative)• Restricted access security controls (preventative)							
Planned Actions							
Residual Impact Score				Residual Likelihood Score			
4				4			
Score Change (since last reporting)	Risk Owner	Action Owner(s)	Target Risk Score	Target Risk Date	4T's		
	Janet Richardson, Professor Paul Knight and Andy McClintock	To be assigned	8		Treat		
Residual Risk Score							
16							



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	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	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	Dealing with economic uncertainty and the impact on forecasting future benefit expenditure and the consequent impact on our administrative budgets and workforce planning
(CR-001) Workforce planning and organisational design			(CR-003a) Value for money
(CR-002) Fraud			(CR-003b) Financial management
(CR-004) Quality			
(CR-005) Performance, culture and inclusion			
(CR-006) Technology and systems			
(CR-007) Safeguarding			
(CR-008) Organisational Resilience		(CR-008) Organisational Resilience	
(CR-009) Delivering for our clients		(CR-009) Delivering for our clients	
(CR-010) Cyber security			
(CR-011) Programme closure			
(CR-013) Protective security	(CR-012) Management information and performance (Data)		(CR-012) Management information and performance (Data)
	(CR-014) Data protection		