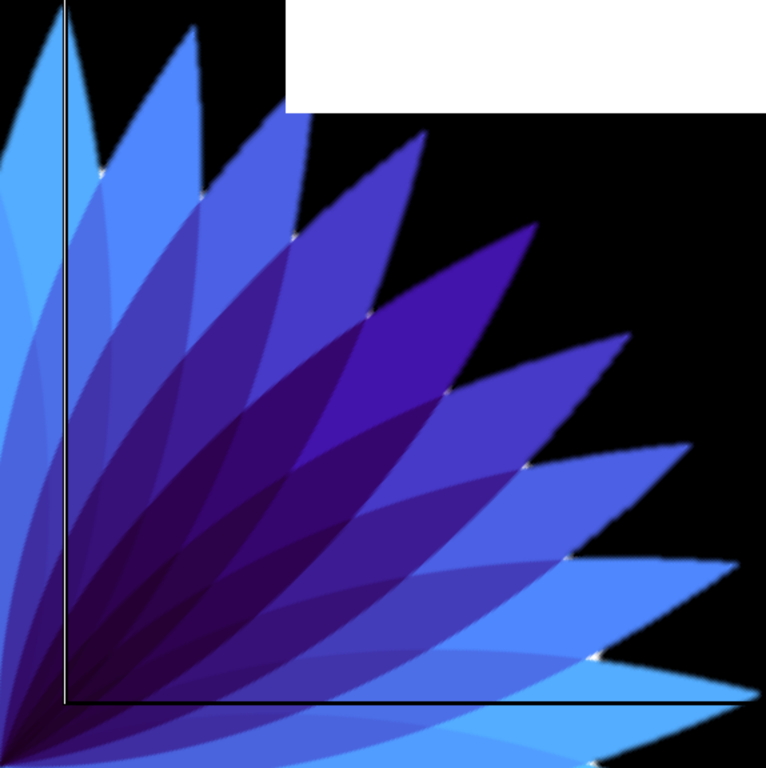
Scottish Government
Riaghaltas na h-Alba
gov.scot

Directorate for Internal Audit and Assurance

Internal Audit Report

Social Security Scotland 2023-24

Role Based Access Controls



Directorate for Internal Audit and Assurance

Issue Date: 2-08-2024

Audit Personnel

Senior Internal Audit Manager:	[redacted]
Internal Audit Manager:	[redacted]
Internal Auditor:	[redacted]
Assurance Support Officer:	[redacted]

Report Distribution

Client Accountable Officer*	David Wallace, Chief Executive
Deputy Director	Andy McLintock, Chief Digital Officer
External Audit*	Audit Scotland
Key Audit contacts	[redacted]
Internal Audit Business Support Hub*	[redacted]

* Final Report only

Contents

1. Introduction

1.1. Introduction

This Internal Audit review of Role Based Access Controls formed part of the Audit Plan agreed by the Accountable Officer and noted by the Audit and Assurance Committee on 21 March 2023. The Accountable Officer for Social Security Scotland is responsible for maintaining a sound system of governance, risk management and system of internal control that supports the achievement of the organisations policies, aims and objectives.

1.2. Audit Scope

The scope of this review was to evaluate and report on the controls in place to manage the risk surrounding Role Based Access Controls for systems utilised by Social Security Scotland. Role Based Access Controls, also known as role-based security, is an access control method that assigns permissions to end-users based on their role within the organisation. Such controls provide a simple, manageable approach to access management that is less error-prone than individually assigning permissions. This review considered the overarching strategy and approach for role-based system access controls across all systems. We then determined what was happening in practice by focussing our testing on SPM, the main system utilised by Social Security Scotland for administering benefits.

It is important to acknowledge that development and delivery of the systems and processes for Social Security Scotland is being undertaken following an agile methodology. [redacted] designed, built, and delivered by Social Security Programme and Policy teams within the Social Security Directorate, with input from Social Security Scotland. Systems and processes are then operationalised by Social Security Scotland. After a period of support and in some instances joint development beyond [redacted] systems and processes will transition to Social Security Scotland with an understanding of live running costs and funding arrangements agreed until the end of the Social Security Programme. Once transitioned, it is the responsibility of Social Security Scotland to make arrangements to improve the systems and processes.

The agreed Terms of Reference for this review is attached at Annex B.

1.3. Assurance and Recommendations

Assurance Category	**Limited**		
Recommendations Priority	**High**	**Medium**	**Low**
	[redacted]	[redacted]	[redacted]

Our review has identified [redacted] priority level recommendations. [redacted]

[redacted] Social Security Scotland's Identity and Access Management Policy is in place, [redacted] A Social Security Scotland wide Identity Access Management strategy was proposed in 2021, [redacted] We believe that implementing our audit recommendations will help mitigate areas of risks that Social Security Scotland is currently facing regarding user access management and controls.

Findings are summarised against recommendations made in the Management Action Plan.

Full details of our findings, good practice and improvement opportunities can be found in section 3 below.

Please see Annex A for the standard explanation of our assurance levels and recommendation priorities.

2. Management Action Plan

2.1. Management Action Plan

Our findings are set out in the Management Action Plan below.

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
1	Identity Access Governance **Issue 1**: [redacted] Social Security Scotland Identity and Access Management Policy is in place and should apply to all systems and users in Social Security Scotland, including colleagues, contractors and affiliates of Social Security Scotland, [redacted] [redacted] **2**: [redacted]	Social Security Scotland should [redacted] implement an IAM strategy [redacted] Once established, local practices and guidance		**Response:** Accepted **Action** • Review and update the Identity and Access Management policy to ensure it covers all users and systems. • We will work with stakeholders to [redacted] Identity and access Management Strategy. The strategy will be taken to Information Governance Group for formal approval and sign off. **Action Owner** - [redacted]	Jan 2025 Oct 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Se[redacted] **Issue 3**: [redacted] **Risk:** [redacted]	should be reviewed to ensure these are appropriate and aligned with the agreed policy and strategy for Identity and Access Management. [redacted] this should reflect Social Security Scotland's access management governance arrangements to ensure access is granted based on role requirements and need.		**Action** - [redacted] **Action Owner:** [redacted]	Oct 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
2	Access Management for IT Administrators **Issue 1**: [redacted] **Issue 2**: We were not able to provide assurance that [redacted] **Issue 3:** We could not evidence that [redacted] The IT Service Catalogue, once complete, ill map out all systems and services used by l Security Scotland and include within	Action should be taken to ensure there are effective processes and guidance in place for [redacted] This should be aligned with overarching policy and strategy. Action should then be taken to ensure all colleagues with [redacted] required for their role. Any access not aligned with policy and role	🟨	**Response:** Accepted **Action** - [redacted]. Work has now started on [redacted] **Action Owner:** [redacted]	Oct 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	that details of ownership, etc. However, at the time of our fieldwork this incomplete. **Risk:** [redacted] **Risk 2:** IT systems do not [redacted]	requirements should be removed. Ongoing action should be taken to ensure those [redacted] To support this process, it is also recommended that management ensure the IT Service Catalogue of all systems and services used by Social Security Scotland is completed, with all relevant details included and this should be maintained so as to provide a complete view of the IT systems and services used by the Agency.	🟨	**Action** - IT Service Management area to regularly review Administration users and ensure access remains appropriate. **Action Owner:** [redacted] **Action:** - IT Service Management area to maintain IT service catalogue for complete view of IT systems and services in use. **Action Owner:** [redacted]	Mar 2025 Mar 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
3	IT Service Design Documentation **Issue**: Of the 286 Live IT Services listed in the Service Catalogue [redacted]. Whilst we recognise that many systems are still owned by Social Security Programme, it is essential such documentation is available to enable the implementation of effective governance and controls. **Risk:** [redacted]	Management should get assurance [redacted] used by Social Security Scotland, is in place to ensure that staff managing access to these services and systems have access to adequate guidance. Where such documentation is not available this should be developed by the relevant party and shared with relevant Social Security Scotland colleagues.		**Response:** Accepted **Action** • Support Technical Platform Owners with required documentation updates that reflect an accurate view of the deployed services within the Social Security Scotland AWS estate. **Action Owner –** [redacted] **Action** • [redacted] **Action Owner –** [redacted] **Action**	Oct 2025 March 2026

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
		This should also be factored into transition to ensure products are not transitioned [redacted]		- We will review existing IT service designs [redacted] **Action Owner –** [redacted] **Action** - We will review service catalogue and report where we [redacted] **Action Owner –** [redacted]	March 2025 March 2025
4	System Target Operating Model **Issue**: A Target Operating Model for [redacted]	Management should develop a Target Operating Model [redacted]		**Response:** Accepted **Action:**	

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	[redacted] **Issue 2:** SPM rolename identifiers [redacted] **Risk:**	[redacted]		Prepare and agree a high level plan setting out key milestones to addressing the recommendations of the Audit to be presented to the Executive Group for agreement and prioritisation. The plan will set out the first step as the need to conduct pre discovery work to understand the scope and complexity of the challenge to inform actions with a formal update of pre discovery progress and any short-term wins provided back to the audit team within 3 months. **Action Owner:** CDO Senior Management Team	October 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	There is a risk that [redacted]	[redacted] Similar action should be taken in relation to other Social Security Scotland systems [redacted]			
5	IT Service Desk Provision of System Access **Issue 1**: [redacted] **Issue 2**:	Both guidance documents referred to in our findings should be reviewed, updated as necessary and once complete be finalised and then implemented to ensure a clear and consistent approach to providing system access by the IT Service Desk.		**Response:** Accepted **Action:** - We will finalise guidance documents for creating & enabling [redacted] **Action Owner:** [redacted]	March 2025

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	IT Service Request Management guidance is [redacted] **Issue 3:** From our substantive testing of SPM user accounts, [redacted] **Issue 4:** Our review [redacted]	As part of this arrangements for [redacted]	🟨		

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Risk: [redacted] **Risk:** [redacted]				

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
6	User Access Reviews **Issue:** Whilst we were advised there were processes in place for conducting User Access Reviews to [redacted] [redacted] **Risk:**	Management to review arrangements for undertaking User Access Reviews for systems used by Social Security Scotland and ensure that this is included in relevant policy/guidance/standard operating procedures. It should be ensured that as well as detecting and taking action [redacted]	🟨	**Response:** Accepted **Action:** We will review User Access Review processes for all systems. **Action Owner:** [redacted] **Action:** Subject to resourcing provision we will put in place a dedicated access management team. **Action Owner:** [redacted]	March 2025 March 2026

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Processes and procedures for conducting user access reviews [redacted]		🟨		
7	Onboarding arrangements **Issue:** Social Security Scotland Onboarding Team and Chief Digital Office both have their own process/procedure for requesting new user accounts. **Risk:** Arrangements for onboarding are not unified across the organisation resulting in duplication of efforts, ineffective way of working and inefficient use of resources.	Management to review the need for having two onboarding teams within the same organisation (Social Security Scotland Onboarding Team and Chief Digital Office Onboarding Team) to ensure that arrangements in place do not result in duplication of efforts, ineffective way of working and in an ineffective use of resources.	🟨	**Response: Accepted** **Action:** • We will review the need for two onboarding teams. **Action Owner –** [redacted]	March 2025

3. Findings, Good Practice and Improvement Opportunities

3.1. Good Practice

3.1.1. There is an established governance process for [redacted]

3.1.2. Social Security Scotland employs [redacted]

3.1.3. Controls are in place to ensure user access accounts are disenabled when staff leave Social Security Scotland. This includes a mandatory process for managers to follow for staff leaving (permanent, temporary and contractors) or transferring elsewhere in the Scottish Government and for internal moves.

3.1.4. We were provided with data on staff who had left Social Security Scotland during the period April 2023 – February 2024; we confirmed appropriate action had been taken with the 178 leavers accounts as all were no longer active.

3.2. Improvement Opportunities

Identity Access Governance

3.2.1. Social Security Scottland's Identity Access and Management Policy is in place and sets out roles and responsibilities for the Chief Digital Officer, Risk and Assurance Manager, Information Asset Owners, line managers and users. [redacted]. **Recommendation 1**

3.2.2. [redacted]

[redacted]

3.2.3. We would like to highlight good practice within the proposal as it includes details on what Identify Access Management is, why it is important to Social Security Scotland, and it recognises that the existing mechanisms for managing colleague access to systems [redacted] **Recommendation 1**

3.2.4. Amazon Web Services (AWS), the platform that hosts Social Security Scotland's benefit applications, contains a built in Identity and Access Management web service that provides guidance on how to securely control access to AWS resources. [redacted] **Recommendation 1**

Access Management for IT Administrators

3.2.5. [redacted] **Recommendation 2**

3.2.6. [redacted] This is primarily

due to the IT Service Catalogue, the document that maps out all systems and services used by Social Security Scotland, being incomplete [redacted]

Recommendation 2

[redacted]

3.2.7. Of the 286 Live IT Services listed in the Service [redacted]

We recognise that the ownership for most of the systems/services used by Social Security Scotland still sits with Programme, however, Social Security Scotland should seek assurance that appropriate system documentation is put in place as staff in Social Security Scotland are asked [redacted]

Recommendation 3

SPM Target Operating Model

3.2.8. A Target Operating Model for system security roles within Social Security Scotland [redacted]

[redacted]

Recommendation 4

- [redacted]

  [redacted] 4

IT Service Desk Access Management

3.2.9. Creating & Enabling of SPM accounts V0.7 October 2022 is the guidance document setting out the established process for requesting/managing access and also detailing the process within the Social Security Scotland IT Service Desk for enabling SPM accounts. [redacted] the IT Service Desk approach is appropriate and key segregation of duties are maintained. **Recommendation 5**

3.2.10. IT Service Request Management guidance is currently in draft with the aim to capture how IT Service Desk Requests are handled with step-by-step requirements, including requests for access rights. The process needs to be alised [redacted]

[redacted] We would advise that this process is reviewed/approved by the Social Security Scotland Chief Information Officer to ensure that it meets needs of the Identity Access Management policy and best practice. Recommendation 5

3.2.11. The process for requesting access rights is reliant on Line Managers providing details of an individual's systems access requirements and on IT Service Desk to grant these access rights. [redacted]

3.2.12. We were provided with data on staff who had joined or moved role within Social Security Scotland for the period April 2023 – February 2024; there were 349 Joiners and 867 movers. We were able to confirm individuals accounts were enabled within SPM [redacted] Recommendation 5

3.2.13. [redacted]. Recommendation 5

User Access Reviews

3.2.14. [redacted]

[redacted] **Recommendation 6**

3.2.15. We were provided with data of SPM Application users dated 11 March 2024; the file had a total of 5,110 entries. [redacted]

3.2.16. However, our analysis of SPM Application Users' Logins in the previous 100 days identified [redacted]. **Recommendation 6**

Onboarding Arrangements

3.2.17. Social Security Scotland's HR Onboarding Team and the Chief Digital Office both have their own process/procedure for requesting user accounts. We note that management should review arrangements for having two onboarding teams within the same organisation and evaluate whether processes are aligned, whether any duplication of efforts exists and whether having two separate teams is effective use of resources. **Recommendation 7**

Annex A Definition of Assurance and Recommendation Categories

Assurance Levels

Substantial Assurance **Controls are robust and well managed**	Risk, governance and control procedures are effective in supporting the delivery of any related objectives. Any exposure to potential weakness is low and the materiality of any consequent risk is negligible.
Reasonable Assurance **Controls are adequate but require improvement**	Some improvements are required to enhance the adequacy and effectiveness of procedures. There are weaknesses in the risk, governance and/or control procedures in place but not of a significant nature.
Limited Assurance **Controls are developing but weak**	There are weaknesses in the current risk, governance and/or control procedures that either do, or could, affect the delivery of any related objectives. Exposure to the weaknesses identified is moderate and being mitigated.
Insufficient Assurance **Controls are not acceptable and have notable weaknesses**	There are significant weaknesses in the current risk, governance and/or control procedures, to the extent that the delivery of objectives is at risk. Exposure to the weaknesses identified is sizeable and requires urgent mitigating action.

Recommendation Priority

High	Serious risk exposure or weakness requiring urgent consideration.
Medium	Moderate risk exposure or weakness with need to improve related controls.
Low	Relatively minor or housekeeping issue.

Annex B – Terms of Reference

Scottish Government
Riaghaltas na h-Alba
gov.scot

Directorate for Internal Audit and Assurance

Internal Audit Terms of Reference

Social Security Scotland 2023-24

Role Based Access Controls

Directorate for Internal Audit and Assurance

Issue Date: 16-02-2024

Key Audit Contacts

Audit Year:	2023-24
Client Accountable Officer:	David Wallace, Chief Executive
Deputy Director	Andy McLintock, Chief Digital Officer
Client Audit Contact(s):	[redacted]
Senior Internal Audit Manager:	[redacted]
Internal Audit Manager:	[redacted]
Internal Auditor:	[redacted]
Assurance Support Officer:	[redacted]

Estimated Reporting Timescale

Fieldwork Starts:	February 2024
Fieldwork Ends:	March 2024
Draft Report Issued:	March 2024
Final Report Issued:	April 2024
Estimated Resource Days:	30

1. Introduction

1.1. This internal audit review of Role Based Access Controls replaces the Embedding and Enhancement review which formed part of our planned audit coverage agreed by the Accountable Officer and noted by the Audit and Assurance Committee on 21 March 2023.

1.2. It is important to acknowledge that development and delivery of the systems and processes for Social Security Scotland is being undertaken following an agile methodology. [redacted] designed, built, and delivered by Social Security Programme and Policy teams within the Social Security Directorate, with input from Social Security Scotland. Systems and processes are then operationalised by Social Security Scotland. After a period of support and in some instances joint development beyond [redacted] systems and processes will transition to Social Security Scotland with an understanding of live running costs and funding arrangements agreed until the end of the Social Security Programme. Once transitioned, it is the responsibility of Social Security Scotland to make arrangements to improve the systems and processes.

1.3. As Social Security Scotland continues to grow, new teams are established and home/hybrid working continues, sufficient arrangements to ensure staff have the required access to systems to enable them to undertake their roles need to be in place. These controls need to be balanced with ensuring Social Security Scotland maintains sound controls in relation to information security, data protection and segregation of duties to ensure colleagues only have access to systems, functionality and data which is relevant to their role.

1.4. The review will consider arrangements for Access Management and System Administration including the processes for new system access requests, temporary access, staff changing roles or leaving Social Security Scotland and access for stakeholders external to Social Security Scotland.

1.5. Previous audit coverage has included our 2021/2022 Review of SPM that included System Access and Administration and in October 2022 our review of IT Supply cluded a high-level review of Access Management strategy, policies and dures.

1.6. The following risks have been identified within Social Security Scotland's Strategic Risk Register:

[redacted]

[redacted]

[redacted]

1.7. We held a planning meeting on 21 December 2023 with key contacts to discuss relevant risks and scope of this review. Our key risks below have been developed through this discussion and our knowledge of Social Security Scotland and its objectives.

2. Scope

2.1. To evaluate and report on the controls in place to manage the risk surrounding Role Based Access controls for systems utilised by Social Security Scotland. This review will consider the overarching strategy and approach for role-based system access controls across all systems. We will then determine what is happening in practice by focussing our testing on SPM, the main system utilised by Social Security Scotland for administering benefits.

2.2. **Remit 1 – Governance**

Remit purpose:

To ascertain whether there is an appropriate strategy which establishes the organisations approach to managing access for all systems used by Social Security Scotland and that it contains effective access control procedures.

Key Risks:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted] review process and unauthorised system access going undetected.

2.3. **Remit Item 2 - Business User's Access**

Remit purpose:

To evaluate the effectiveness of business user access controls.

Key Risks:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

2.4. Remit Item 3 – IT Administrator Access

Remit purpose:

To evaluate the effectiveness of IT User/ Administrator access controls.

Key Risks:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

3. Approach

3.1. We will undertake the audit in compliance with the Internal Audit Charter and Memorandum of Understanding agreed between Internal Audit and Social Security Scotland.

3.2. At the conclusion of the audit a customer satisfaction questionnaire will be issued to the main client audit contact. Internal Audit appreciate feedback and to facilitate continuous improvement, we would be grateful if you could complete and return the questionnaire.

3.3. Client is reminded of our need for timely access to people and responsiveness to information requests, to enable the reporting timetable to be met.