Scottish Government
Riaghaltas na h-Alba
gov.scot

Directorate for Internal Audit and Assurance

Internal Audit Report

Social Security Scotland 2022-23

Incident Management

Directorate for Internal Audit and Assurance

Issue Date: 12-04-2023

Audit Personnel

Senior Internal Audit Manager:	[Redacted]
Internal Audit Manager:	[Redacted]
Internal Auditor	[Redacted]

Report Distribution

Client Accountable Officer*	David Wallace, Chief Executive
External Audit*	Audit Scotland
Key Audit contacts	[Redacted]Head of Change and Project Management [Redacted]Live Service Manager [Redacted]Live Service Manager [Redacted]Project Management Office Manager [Redacted], Acting Head of Change and [Redacted], Head of Change & Project Management [Redacted]Change Manager [Redacted]Head of Business Change Management [Redacted]Business Resilience Lead [Redacted], Fraud and Error Systems and Process Lead [Redacted]Social Security Directorate Programme Change Service Manager [Redacted] Social Security Directorate Programme Delivery lead [Redacted]Social Security Directorate Programme Test manager [Redacted]Social Security Directorate Programme Delivery

	[Redacted] Social Security Directorate Head of Release Management, Transition & Lessons Learned
Internal Audit Business Support Hub*	[Redacted]

* Final Report only

Contents

1. Introduction

1.1. Introduction

This Internal Audit review of Incident Management formed part of the Audit Plan agreed by the Accountable Officer and noted by the Audit and Assurance Committee on 25 March 2022. The Accountable Officer for Social Security Scotland is responsible for maintaining a sound system of governance, risk management and system of internal control that support 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 Social Security Scotland's Incident Management arrangements.

To aide understanding, it is important to clearly set out the relationship between Social Security Scotland and the Social Security Directorate (Programme). Social Security Directorate designs and builds the new Scottish social security system and is delivering the components on an incremental day to day basis. As such Minimal Viable Products for policies, systems and processes for each benefit are built by Social Security Directorate, and then handed to Social Security Scotland to deliver. It is then the responsibility of Social Security Scotland to develop these as appropriate to make them fit for purpose and reflecting actual processes and controls in place.

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

1.3. Assurance and Recommendations

Assurance Category	**Reasonable**		
Recommendations Priority	**High**	**Medium**	**Low**
	0	**4**	**1**

Our review has identified four medium and one low priority recommendations. A reasonable assurance rating has been provided. 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.

The rationale for this is that Internal Audit recognises that there are significant processes and procedures in place to manage incidents as they occur, there is room to strengthen and develop these processes to ensure they work more effectively. Internal Audit recognises that some of the challenges faced by Social Security Scotland are as a result of tight timeframes within Programme prior to roll out. However, Social Security Scotland is proactive in continually improving response to these issues and has documentation in place to support these activities.

We note that in order to avoid duplication of work, this audit review placed assurance on work done by the Digital Assurance Office who undertake go live gate reviews on pre-release arrangements. The latest report highlighted issues with the testing, and bad practice in relation to timescales for testing being pushed back limiting the time and ability to do testing prior to release. This includes regression testing, which while highlighted as part of the terms of reference, was then found to be outside the remit of this review as this work sits within Programme exclusively. Recommendations are raised through Digital Assurance Office reports and implementation is monitored.

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	Major Incident Response Framework **Issue**: Sections of the Major Incident Response Framework document relating to major IT Incidents require update to ensure alignment with the management of Priority 1 (P1) incidents. See paragraph 3.2.1. for more detail. **Risk:** Incorrect or conflicting information may result in delays in responding to and managing IT incidents, negatively impacting on payments to customers and/or delays in processing applications.	The Major Incident Response Framework document should be reviewed and updated to ensure it reflects current practices in the management of P1 incidents. Management should ensure such a document is subject to periodic reviews to ensure it remains accurate and up to date and fit for purpose.	**M**	Response: Accepted Action: The Major Incident Framework is currently under review, including the current Officer in Charge process and their role in technical related incidents. The Business Resilience Lead will initiate discussions with required stakeholders to agree clarity and triggers for when the Officer in Charge/Major Incident Framework should be invoked. The updated framework will include links to	Aug 2023

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
				incident materials referenced within section 3.2.1 Once the framework is updated, it will be subject to an annual review (as per other Business Resilience documentation). Action Owner: [Redacted] Business Resilience Team	
2	Chief Digital Office Incident Management Guidance and Processes **Issue 1:** Guidance and documented processes for incident management arrangements in the Chief Digital Office are not always in place, formally reviewed and signed off. See paragraphs 3.2.4 to 3.2.7 for more detail.	a) Guidance and documented processes for incident management arrangements in the Chief Digital Office should be completed and/or reviewed and formally signed off. Appropriate document controls should be used to	M	Response: Recommendations A, B and C accepted Action: a) CDO IT Service Incident/Request/Problem Management Process reviews to allow formal approval / distribution / governance including review	Aug 2023

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Issue 2: Staff are unaware of how priorities are allocated to Jira tickets which have been raised. **Risk:** Lack of clear guidance and processes may result in tickets being allocated inappropriate prioritisation, resulting in delays in response and an inadequate level of service being provided. Staff are unaware of progress against tickets raised and may raise further tickets, resulting in increasing workloads, negatively impacting on the ability to response to tickets effectively.	allow for audit trail of reviews. b) Information on how prioritisation is allocated to Jira tickets should be made available to all Social Security Scotland staff. c) Management should consider if the process for closure of Jira tickets could be made more efficient by Live Service Team having access to do this, where appropriate.		schedule. This will underpin formation of Operations Handbook in addition to providing framework for Local Working Procedures. b) Updated IT Service Incident / Request / Problem Management definitions to include Service Level Target (SLT) information in the revised IT Service Management Process documents. Action Owner: [Redacted] c) IT service desk to review the process regarding update and closure of incidents Action Owner: [Redacted]	

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
3	<u>Incident Communication Plan</u> **Issue:** Whilst Social Security Scotland has adopted the Scottish Government communications process guides, at the time of the fieldwork, we were unable to obtain evidence of there being an agreed Social Security Scotland specific communications approach/plan for incidents. We also noted these process guides were not integrated into the wider Social Security Scotland Major Incident Response Framework and there was limited awareness and understanding of the process outwith the Communications team. During our fieldwork we reviewed the Incident Lessons Learned tracker and this highlighted issues with communications to staff and stakeholders in relation to ongoing incidents.	The communications approach/plan for managing incidents should be reviewed and updated to ensure that this reflects the needs of the Social Security Scotland. Management should ensure that key stakeholders are involved in agreeing the final approach. As part of the review, feedback and lessons learned from previous incidents in relation to communications should be considered.	M	Response: Partially accepted see comments Social Security Scotland has a dotted line into Scottish Government Communications Division. As such, it adopts Scottish Government Communications Division ways of working – including our approach to incident and crisis communications and our sign off processes. When an incident occurs, communication will allocate a lead to be part of the incident response team. They will assess the situation and provide communication advice and then follow existing processes to deliver required communication outputs. The communication team	June 23

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Risk: The communications approach to incidents is ineffective, action taken is inconsistent and disjointed across teams in Social Security Scotland and relevant staff and stakeholders not being made aware of incidents which have occurred, resulting in duplicate tickets being raised unnecessarily and inconsistencies in messaging and engagement leading to reputational damage and impacting negatively on staff morale.	The final approach should be integrated in the Major Incident Response Framework and communicated to all those involved in incident management activities.		have a good understanding of their roles and responsibilities and processes. We accept that the existing communication processes are not widely understood by others involved in the incident response. To resolve this, we will develop a short overview of the communication approach to incidents to be included within Social Security Scotland incident documentation. This will include clarity on roles and responsibilities. Sign off processes are well established and are widely used across Scottish Government and its agencies. These move at pace when required. All steps in these	

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
				processes are required to ensure communication activity is appropriate and accurate and doesn't create other unintended risks or issues. Action: Action Owner: [Redacted] External Communications Team Leader (Corporate)	
4	<u>Lessons Learned</u> **Issue:** Lessons learned processes are disjointed and not appropriately centralised. **Risk:** Lessons learned may not be adequately captured and reflected across the organisation, failing to demonstrate	Consideration should be given to centralising the lessons learned process for incident management to ensure all relevant lessons are captured and planned improvements monitored and rolled out across delivery.	M	Response: Accepted Action: Lessons learned process already established. Business Resilience Lead has linked with Agency Lessons Learned Lead and has agreed to shadow some future lessons learned event. In order to	Jun 2023

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	improvement, not be subject to appropriate scrutiny and implemented as needed.	Appropriate scrutiny should be in place to help ensure that activities are prioritised in line with business needs.		upskill and facilitate session following a major incident Support will also be provide when needed from the Agency Change Manager. Action: work is currently ongoing by the Business Resilience Team to streamline process for lessons identified from incidents. Agreement should be made by key stakeholders as to how lessons identified are made visible, prioritised, and progressed accordingly – and aligned with other lessons learned existing processes. Action Owner: [Redacted]	
5	<u>Compliance with Major Incident Guidance</u> **Issue:**	Management should ensure sufficient controls	L	Response: Accepted	Jun 2023

No.	Issue & Risk	Recommendation	Priority	Management Response & Action Owner	Action Date
	Post Incident reports, Incident Logs and Lessons learned/feedback forms are prepared by Officers in Charge for all Major Incidents. These are collated by the Business Resilience Team, however, no tracker is in place to ensure that reports and incident logs were completed as per official guidance. **Risk:** Failure to complete documentation in line with guidance may result in inaccurate records, inappropriate closure of incidents and an inability to capture all lessons learned and ensure remedial action is taken to enable continuous improvement in relation to incident management.	are in place to ensure that all reports and logs for major incidents are completed in line with the Major Incident Response guidance. Exceptions to this should be examined. Roles and responsibilities for this should be formally assigned.		Action: The Business Resilience Team have recently created an excel sheet to track paperwork for all incidents, to ensure all necessary logs are returned by relevant response team members. A process for non-returns will be determined and documented within the next version of the Business Continuity framework. Action Owner: [Redacted] Business Resilience	

3. Findings, Good Practice and Improvement Opportunities

3.1. Good Practice

Remit 1 – Pre-release governance arrangements

3.1.1. Responsibility for the development of releases to be applied to systems lies within Programme. Social Security Scotland participate in release management processes and this engagement generally starts around 12 weeks out from release. This involves ensuring that the Release Managers understand the scope being released at an early stage. Immediately after release, a 'Hypercare' system is implemented while upgrades bed into a steady state. The length of time this is provided for is normally between six weeks and six months. There is documented guidance in place for this and work is ongoing to ensure this works effectively. Social Security Scotland is notified of potential issues from Programme prior to roll-out. Broadly, Social Security Scotland agree which defects can be put into live with the various releases. Impact testing will be undertaken to inform management and enable agreement of which ones are acceptable and which ones are not.

3.1.2. The first phase of the Hypercare support is implemented during the 'Go Live Weekend', with establishment of a Jira Board (This displays the team's work as cards you can move between columns. In Jira Software, cards and the tasks they represent are called "issues". The Jira Board aligns with the team's processes and allows for tracking the status of each issue as it makes its way through the team's process, ready for defect creation.). There is agreement around how tickets should be raised. This includes a prefix to identify if incidents raised relate to the release. It is not always clear which incidents are related to release, however, when raised they go through a triage for the technical team to assess if linked. The prefix can then be amended to the correct one. There is then a Post Hyper Support Period, which is in place for six to eight weeks, dependent on the size and scale of the release. This enables issues to be raised by Social Security Scotland to be managed in conjunction with Programme. After this point, the management of outstanding issues will be handed to Social Security Scotland to manage, dependent on the type of issue. There is a one-week handover period for this. After the Hypercare period the standard Social

Security Scotland Incident Management process is utilised to manage any incidents that occur.

3.1.3. The terms of reference for this review highlighted that review of regression testing would also be undertaken, however, this fell outside the remit of this review as responsibility for this sits within Programme. As detailed below the Digital Assurance Office (DAO) division within the Directorate for Internal Audit and Assurance has undertaken work in this area and Internal Audit will be placing reliance on this, rather than reperforming the work completed by this team.

3.1.4. In addition, Internal Audit previously undertook a review of Social Programme Management (SPM), the client management system used for the administration of benefits delivered by Social Security Scotland. Within this a recommendation was made in relation to the timescales in place around testing and the need to strengthen this process. The recommendation was accepted by management, with a proposed implementation date of March 2023. Follow-up work is planned at a future date where we will review action taken. As such, no further work was undertaken in relation to this as part of this review.

3.1.5. The Chief Digital Office Risk Register shows evidence of regular review and captures immediate risks to delivery, including those relating to release of rollout of new benefits/system upgrades. It is Internal Audit's opinion that this risk register is fit for purpose, adequately captures all risks, evidences regular maintenance, and demonstrates ongoing management and mitigation of risks and issues. Updates on risk through presentations are provided to the Chief Digital Officer. There is also a risk working group with a consistent and regular agenda and the attendee list represents an appropriate cross section of individuals across Social Security Scotland involved in Chief Digital Office.

3.1.6. There is a clear process in place for escalation of risks. Internal Audit found this to be a complex process, with checks and balances in place. However, the clarity supports appropriate escalation and management of these risks. Internal Audit is content that there is sufficient processes in place to identify and manage risks and issues relating to issues and updates to the system.

3.1.7. Due to issues occurring as a result of roll out of upgrades to the system, the Testing Team undertook some analysis on the issues to identify the key risks and how these can be managed effectively. During the review a number of findings were made, with recommendations identified to better support and manage roll out, as well as improving the response to any issues that occur as a result of these upgrades. It is Internal Audit's opinion that this demonstrates the team are being proactive in identifying risks and issues and in identifying ways to improve delivery and management.

Remit 2 – Incident identification, classification and management

3.1.8. The Social Security Scotland Major Incident Response Framework confirms the Major Incident Response Group and the key stakeholders responsible for implementing and managing the incident management process. This information is confirmed within the Problem Management process and within the draft Chief Digital Office Incident Management process.

3.1.9. Members of the Chief Digital Office Live Service Team meet with members of the IT Service Desk team on a weekly basis to discuss working arrangements between both teams and to identify improvements in relation to SPM. Actions from these meetings are monitored to ensure implementation.

3.1.10. Weekly team sessions are held by the Chief Digital Office Live Service team to allow for team support in managing and resolving complex incidents. This also allows for a discussion of best practice and areas for improvement.

Reporting and intervention

3.1.11. Root cause analysis is undertaken for major incidents and corrective actions are identified, tracked, and updated as part of monthly Chief Digital Office IT Service reports. Problem Reports are prepared to summarise the root cause analysis for major incidents, and these are shared with key stakeholders. The Chief Digital Office Major Incident Manager is undertaking analysis on the most common IT failures /incidents reported in order to develop and identify preventative measures with an aim of decreasing incidents/IT failures.

3.2. Improvement Opportunities

Incident identification, classification and management

3.2.1. All major incidents raised through the Jira portal classified as Priority 1 (P1) incidents, trigger an organisational wide major incident response in line with the Major Incident Response Framework that is owned by the Business Resilience Team. Internal Audit found that:

- The framework requires finalisation, review and sign off by all key stakeholders in the incident management process.
- Biannual requirement for review is stated within the framework, with last review of the document recorded as 2021. Internal Audit has noted that some key personnel are no longer in post. (e.g. the named IT Service Desk Manager)
- Localised incident response plans (Chief Digital Office Incident Management Process, Chief Digital Office Problem Management process, IT Service Desk Major Incident Identification process, Finance Incident Response process, etc) should be included in the framework as annexes to fully reflect the organisation's approach to incident management.

3.2.2. Internal Audit recognises that the Major Incident Response Framework covers all aspects of business recovery, not just that relating to major IT incidents. Internal Audit would recommend that the sections applicable to the management of major IT incidents be reviewed in full to ensure alignment with the management of P1 incidents. **(Recommendation 01)**

3.2.3. The Social Security Scotland Major Incident Response Framework highlights the prioritisation of activities while recovering from an incident. It also includes details of the teams that are instrumental in Social Security Scotland's ability to deliver benefits when recovering from an incident. However, at the time of our review, analysis to determine the activities and teams that should be given priority during disruption have not been identified. This is a gap that should be addressed to support delivery of priority activities during any disruption. **(Recommendation 01)**

3.2.4. Guidance and documented processes for incident management arrangements are not always in place, formally reviewed and signed off. This includes:

- The Chief Digital Office Problem Management process – No evidence of formal review and sign off. The document refers to a 'Problem Board' which has not been established.
- The Chief Digital Office Incident Management process – Document details that this was last reviewed in 2019. Internal Audit notes that a review of this has now commenced, including supplementary documentation, such as templates.
- The Chief Digital Office Live Operations Handbook and associated incident management guidance are still to be completed.
- The IT Service Desk One Note included incident management guidance that differed to the versions provided to Internal Audit by the Chief Digital Office Major Incident Manager. Internal Audit also notes that the guidance on OneNote does not show evidence of review since 2020 and there is a risk that this does not reflect current processes.

3.2.5. It is Internal Audit's opinion that the current IT Service Desk process for identifying Major Incidents (P1 and P2s) requires improving. At the time of the review, there was no guidance in place for IT Service Desk administrators who triage incoming tickets, therefore Internal Audit is unable to comment on the effectiveness of the initial stage of the Incident Management process. Internal Audit would recommend that guidance is put in place to enable identification of major incidents in a timely manner**.** In addition, current system functionality does not allow for analysis of the number of users impacted by a particular outage. This would provide support in classifying incidents and would enable better communication to staff. **(Recommendation 02)**

3.2.6. There is no guidance available to all staff which details how Jira tickets are classified and prioritised. Management may wish to consider introducing an automated response once the ticket is allocated a priority, to provide assurance that the issue is being managed and to enable understanding of priority allocation. **(Recommendation 02)**

3.2.7. The Chief Digital Office Live Service Team currently pass resolved incidents/Jira tickets back to the IT Service Desk to be closed. As the IT Service Desk is currently managing large volumes of tickets, management should consider whether there may be a way for the Chief Digital Office Live Service Team to update and close incident tickets rather than creating a new ticket confirming resolution. **(Recommendation 02)**

3.2.8. Social Security Scotland have adopted the Scottish Government communications process guides. From our review of these guides, we note that these contain reference to the Scottish Government and do not reflect bespoke arrangements within Social Security Scotland. We also noted these process guides were not integrated into the wider Social Security Scotland Major Incident Response Framework and there was limited awareness and understanding of the processes outwith the Communications team. The Framework referred to a Major Incident Communications strategy, however, no detail was included in the annex. During our fieldwork we reviewed the Incident Lessons Learned tracker and this highlighted themes around delays in communicating issues and incidents to staff and stakeholders.

3.2.9. The communications approach/plan for managing incidents should be reviewed and updated to ensure that this reflects the needs of the Social Security Scotland. Management should ensure that key stakeholders are involved in agreeing the final approach. As part of the review, feedback and lessons learned from previous incidents in relation to communications should be considered. The final approach should be integrated into the Major Incident Response Framework and communicated to all those involved in incident management activities.

3.2.10. The plan/approach should make it clear who has responsibility for such communications, what their roles and responsibilities are, the means of communication to be used (e.g. lines to take, Interactive Voice Recording, Staff Communications, Group Call, ministerial messaging, social media, mygov website, etc.), the route for agreement and sign off and timescales for communicating.
(Recommendation 03)

Reporting and Intervention

3.2.11. The process for gathering lessons learned is embedded in the Major Incident Management Process and while lessons learned and corrective actions are identified on multiple levels within the organisation, the processes in place suggest silo working and lack of coordination. There is currently no working group/panel in place to scrutinise efforts and ensure that any corrective actions identified are appropriately prioritised and actioned. We note that this weakness has already been identified by the Business Resilience Manager and escalated to the Agency Leadership Team. Internal Audit would recommend that processes be implemented to centralise this process. **(Recommendation 04)**

3.2.12. Reporting processes are still being developed and are currently manual, time consuming and prone to human error with only some dashboard reporting available through the existing Chief Digital Office IT Service Desk management systems. This impacts the ability to obtain information efficiently and effectively. A review to determine whether current reporting output is fit for purpose has not been completed. This was highlighted in the Internal Audit review of IT Supply in 2022, therefore a formal recommendation will not be made here.

3.2.13. Post Incident reports, Incident Logs and Lessons learned/feedback forms are prepared by Officers in Charge for all Major Incidents. These are collated by the Business Resilience team. As part of our fieldwork, we tried to obtain evidence that for a sample of incidents the required documentation had been completed and processes appropriately actioned with lessons captured and actions taken to progress and implement these, however, due to lack of a tracker or other relevant process, we were not able to review and therefore cannot confirm that in all cases the required documentation and activities are completed as required. **(Recommendation 05).**

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 2022-23

Incident Management

Directorate for Internal Audit and Assurance

Issue Date: 28-09-2022

Key Audit Contacts

Audit Year:	2022-23
Client Accountable Officer:	David Wallace, Chief Executive
Client Audit Contact(s):	[Redacted], Head of Change and Project Management [Redacted], Live Service Manager [Redacted]Live Service Manager [Redacted], Project Management Office Manager [Redacted], Acting Head of Change and Project Management [Redacted] Head of Change & Project Management [Redacted] Change Manager [Redacted] Head of Business Change Management [Redacted] Business Resilience Manager [Redacted] Fraud and Error Systems and Process Lead [Redacted] Social Security Directorate Programme Change Service Manager [Redacted] Social Security Directorate Programme Delivery lead [Redacted] Social Security Directorate Programme Test manager [Redacted] Social Security Directorate Programme Delivery [Redacted], Social Security Directorate Head of Release Management, Transition & Lessons Learned
Lead Senior Internal Audit Manager:	[Redacted]
Internal Audit Manager:	[Redacted]
Internal Auditor	[Redacted]

Estimated Reporting Timescale

Fieldwork Starts:	September 2022
Fieldwork Ends:	October 2022
Draft Report Issued:	November 2022
Final Report Issued:	November 2022
Estimated Resource Days:	30

1. Introduction

1.1. This internal audit review forms part of our planned audit coverage set out in our Annual Internal Audit plan issued on 25 March 2022 and agreed by the Accountable Officer and noted by the Audit and Assurance Committee.

1.2. We have been advised by management that Social Security Scotland has recently encountered a number of incidents in relation to SPM, some of which were as a result of new releases having an impact on live benefits already being delivered. New releases include the introduction of new benefits as well as change and development activity. In each instance Social Security Scotland has had to manage the incident and take action to remedy the situation. Each incident has had an impact on teams across the organisation where business continuity actions have had to be taken, putting colleagues under increased pressure and having to deviate from their usual activities in order to ensure continued delivery and payment of benefits to clients. As such we propose to undertake a review to assess the pre-release arrangements, including consideration of regression testing and controls around non-production environments which are used, the impacting and acceptance process of testing outcomes prior to release, in relation to currently live benefits (excluding Adult Disability Payment), the post release incident management arrangements and the lessons learned activities in order to identify root cause of such issues and minimise the likelihood of them happening again.

1.3. The Social Security Scotland Strategic Risk Register includes the following risk:

- IF there is no formal Business Continuity Management System in place THEN any incident that requires its plans to be invoked will depend on reactive management to resume services RESULTING IN significant reputational damage, impact to client service delivery, impact on health, safety and wellbeing of our people, significant financial implications and failure to meet statutory obligations.

- IF appropriate Change Control/Change Management (as a function) processes are not in place THEN we may fail to land new benefits safely,

assess impact on current benefits and fail to influence future launches RESULTING IN financial loss and missed/delayed client payments leading to sub-optimal staff and client experience.

1.4. We met with [Redacted] Head of Change and Project Management; [Redacted] Project Management Office Manager; [Redacted], Live Service Manager and [Redacted], Social Security Scotland Corporate Assurance Team, on 25th July 2022 to discuss relevant risks and agree the details of this review. Our key risks below have been developed through these discussions 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 Social Security Scotland's Incident Management arrangements.

2.2. Remit Item 1 – Pre – release governance arrangements
To assess whether Social Security Scotland has established appropriate governance arrangements for the consideration, impacting, acceptance and sign-off of risks and issues identified as part of pre-release testing and that mitigating action has been implemented as part of Social Security Scotland's readiness activities prior to new releases going live on SPM.

Key Risks:

- A failure to establish appropriate acceptance and sign off procedures prior to release leading to mitigating processes and controls not being developed and implemented prior to releases resulting in Social Security Scotland not being ready and live benefits being negatively affected.
- Lack of arrangements for understanding the impact of system deficiencies/weaknesses, leading to an inability to make an informed decision as to whether Social Security Scotland is ready and prepared for such impacts and able to accept the update in its current form.
- Insufficient processes established for recording and managing risks and issues inherited as a result of the go live of new benefits, change activity or system updates that have deficiencies/weaknesses.

2.3. Remit Item 2 – Incident Identification, classification and management

To determine if the systems, processes and controls are appropriate for identifying and classifying issues as incidents and the processes for managing such incidents through to recovery.

Key Risks:

- Process for identify issues and appropriately classifying incidents is inefficient or ineffective leading to incidents not being suitably prioritised and managed and corrective action not being taken in a timely manner.
- Social Security Scotland does not have effective processes for managing such incidents impacting the organisations ability to continue to deliver benefits resulting in poor service delivery, financial hardship of clients and reputational damage.
- Appropriate colleagues are not involved in the incident management activities or aware of the recovery actions required leading to inconsistent/inefficient incident management approach and an inability to effectively recover.
- Social Security Scotland does not have the capacity and/or capability and has insufficient support to understand what is impacted in such incidents, identify a solution and implement this resulting in Social Security Scotland being able to effectively manage such incidents and recover leading to an inability to achieve strategic objectives and deliver services.

2.4. Remit Item 3 – Reporting and intervention

To assess the processes and controls in place to report incidents to relevant teams within Social Security Scotland to ensure any action required to resolve and correct benefit processing and payment administration is understood, impact known and action taken.

Key Risks:

- Failure to report incidents for corrective action resulting in clients not obtaining benefits they are due, increased financial loss due to overpayments not being rectified in a timely manner and reputational damage.
- Lack of process to understand impact of corrective actions and the resulting impact on the teams responsible leading to failure to achieve team and

business objectives resulting in diminished service levels and poor quality output impacting client satisfaction and reputation.

- Lessons are not learned, captured and communicated resulting in the same issues recurring.

3. Approach

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

3.2. Due to current Scottish Government remote working requirements, this review will utilise eRDM Connect for sharing documents and screen sharing technology as necessary. It has also been agreed that some elements of fieldwork would be done onsite. Methods of undertaking fieldwork will be amended as appropriate.

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

3.4. 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.