# Directorate for Internal Audit and Assurance

## Internal Audit Report

## Social Security Scotland 2023-24

## Risk Management

Directorate for Internal Audit and Assurance

**Issue Date**: 26-04-2024

## 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 |
| **Deputy Director** | Ally Macphail, Deputy Director, Organisational Strategy and Performance<br>James Wallace, Deputy Director Finance and Corporate Services |
| **Key Audit contacts** | [Redacted] Head of Strategy and Corporate Support<br>[Redacted] Risk and Assurance Team Leader<br>[Redacted] Risk Team Manager<br>[Redacted] Deputy Programme Manager, Social Security Directorate<br>[Redacted] PMO Risk, Issue and Measurable Improvements Manager, Social Security Directorate |
| **Internal Audit Business Support Hub*** | DIAABusinessSupportHub@gov.scot |

* Final Report only

## Contents

# 1. Introduction

## 1.1. Introduction

This Internal Audit review of Risk Management 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 organisation's policies, aims and objectives.

As with all organisations, Social Security Scotland faces risks that threaten the achievement of its strategic objectives, as well as challenging operational risks and risks associated with the protection of its people, property and reputation. Social Security Scotland therefore needs to have an effective risk management approach to safeguard its objectives, which is aligned to its risk appetite and is actively supporting decisions made in the achievement of its objectives.

## 1.2. Audit Scope

The scope of this review was to evaluate and report on Social Security Scotland's Strategic Risk Management arrangements, the controls in place to identify, record, manage/mitigate and report on risks facing the organisation along with the arrangements for management of issues.

It is appropriate to note that development and delivery of the systems and processes for Social Security Scotland is being undertaken following an agile methodology. As such Minimal Viable Products (MVPs) for policies, systems and processes for each benefit are 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 MVP, 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. This working relationship can lead to risks and issues, that may not be within Social Security Scotland's desired risk tolerance and risk appetite, being passed onto the organisation as products are transitioned from Programme

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** |
| | **1** | **4** | **2** |

Our review has identified one high, four medium and two low 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 while significant improvement has been noted in relation to strategic risk management, some gaps in the guidance, training, reporting and oversight processes were identified. In many of these cases, management is already aware and working towards finalising these.

The process for strategic issue management is still to be reviewed and formally signed off and any appropriate strategy, policy, and guidance yet to be put in place, with the focus until now being on the strategic risk management process. As such it is key that management progress with agreeing their approach to strategic issue management. Once agreed any relevant strategies, guidance and processes should be developed and implemented to ensure strategic issues are effectively managed with appropriate governance and oversight in place.

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 | Roles and Responsibilities<br>**Issue**: There is limited information on the Risk Team on Saltire representing a missed opportunity to highlight to the wider organisation the roles and responsibilities of the team, how it is there to support the organisation, as well as containing guidance (once finalised) and links to training on Pathways.<br>**Risk:** Poor understanding and awareness of risk within Social Security Scotland leading to a failure to adequately embed the appropriate risk management practices. | The Risk Team should consider updating and expanding the information on Saltire to include its roles and responsibilities, the support offered, copies of guidance and links to training opportunities to raise awareness of, and embed, the risk management processes across the organisation. | **L** | **Response:**<br>Recommendation accepted.<br>**Action:**<br>Action will be taken in conjunction with our communication team to increase risk management information available on Saltire.<br>**Action Owner:**<br>Risk and Assurance Team Leader | May 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| 2 | Roles and Responsibilities<br>**Issue**: The Terms of Reference for the Executive Team is in draft form and awaiting approval, therefore the Team's roles and responsibilities for strategic risk management are still to be confirmed.<br>The Terms of Reference for the Risk Review Group contains references to the Agency Leadership Team which is no longer in place, this is also depicted in a diagram which shows the previous governance structure of Social Security Scotland (similar diagrams are also in the Risk Handbook and Risk Framework).<br>**Risk:** Appropriate roles and responsibilities, lines of reporting and accountability for strategic risk management have not been | Management should ensure that the Terms of Reference for the Executive Team is finalised, to confirm its roles and responsibilities for risk management.<br>The Risk Team should also ensure that policies and guidance are updated to reflect that the Agency Leadership Team has been disbanded, and these reflect the updated reporting lines. | **L** | **Response:**<br>Recommendation Accepted.<br>**Action:**<br>The risk management team will review and amend all documents, including the Terms of Reference for Risk Review Group, to reflect the current governance structure.<br>The Terms of Reference for the Executive Team will be reviewed by our Governance Team.<br>**Action Owner:**<br>Risk and Assurance Team Leader | May 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | established and embedded across the organisation. | | 🟩 | | |
| 3 | Documented Processes<br>**Issue**: The Risk and Issue Management Framework, Risk Strategy and Risk Team Handbook were under review during our fieldwork. These should be completed and updated to reflect current and future arrangements and should then be shared with appropriate stakeholders.<br>Review of these documents and discussions with staff highlighted that they could be enhanced with the addition of:<br>- Explaining the arrangements for cross referencing risks and sharing of information between Social Security Scotland and Social Security Programme; | Management should review these documents to ensure that they represent and detail the full process undertaken in respect of strategic risk management and thereafter ensure that they are published, shared with appropriate stakeholders and embedded as business as usual. Requirements for ongoing review should be stated to ensure documents / processes remain | M | **Response:** Recommendation Accepted<br>**Action:**<br>The Risk Framework, Strategy and handbook will be reviewed and updated – August 2024<br>Risk Management reporting to the Executive Team and other appropriate governance forums is in development. Work on this will be completed by August 2024.<br>The effectiveness of controls will be discussed with risk owners and as part of Executive Team Risk discussion. As above this will be in place by August 2024. | August 2024<br>August 2024<br>August 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
|  | - Detailing the process for removal or closure of risks;<br>- Highlighting that mitigating controls should clearly set out the key controls and include timescales i.e. when the target risk score is anticipated to be achieved;<br>- Setting out 'what good looks like' to allow evaluation, scrutiny and challenge of mitigating actions and controls;<br>- Documented process for ensuring that the output of the strategic risk management process is utilised in business planning and decision making.<br><br>**Risk 1:** Insufficient and/or ineffective strategic risk management strategy, policy, guidance and training.<br>**Risk 2:** Insufficient and/or ineffective arrangements for oversight and scrutiny of risk | current and effective in driving the risk management activities in Social Security Scotland. | 🟨 | Strategic risks were presented and considered as part of the prioritisation activity for this year's business plan and forward corporate plan. An initial mapping between the draft business priorities and strategic risks was prepared and shared with Executive Team. This mapping will be updated in advance of finalising the business plan for 2024/5 and longer-term corporate plan.<br><br>**Action Owner:**<br><br>Corporate Assurance and Risk Team Leader |  |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | management activities, identified risks and mitigating actions and controls.<br>**Risk 3:** Lack of review of the effectiveness of identified mitigating actions.<br>**Risk 4:** Risk management output not being utilised effectively to ensure decisions are risk based and risk management is embedded in business planning and decision making leading to inappropriate decisions being made and an inability to take advantage of opportunities arising. | | | | |
| 4 | Risk Management Approach<br>**Issue**: Guidance and approach to establishing risk appetite and tolerance levels have not been captured.<br>Risk appetite and tolerance levels have not been set. | Management should set out a process for determining risk appetite and risk tolerance, and ensure that levels for each are set. | M | **Response:** Recommendation Accepted<br>**Action:**<br>We will undertake an initial and ongoing appetite and tolerance setting sessions with our Executive Team. We will then publish risk appetite statements which will be regularly reviewed. | August 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | Whilst the strategic risk register mainly follows risk management best practice, not all risks are written in line with the risk management guidance with some being worded more like statements.<br>Mitigation actions for strategic risks and current controls and mitigations for divisional risks are worded inconsistently and the field that outlines 'planned action to achieve target risk score' was not completed for all risks (see 3.2.11 for details).<br>**Risk:** Inappropriate approach and methodologies for identifying, recording and managing risks. | Additionally, consideration should be given to ensuring a consistent approach is implemented for articulating strategic risks to ensure these can be understood.<br>A review of the strategic risk register should also be carried out to ensure that it is worded and completed consistently and fully. | 🟧 | We will review the wording of our strategic risks and mitigations to ensure these are complete and consistent.<br>**Action Owner:**<br>Corporate Assurance and Risk Team Leader | June 2024 |
| 5 | Issue Management Approach | Management should review the approach to | H | **Response:**<br>Recommendation Accepted | August 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
|  | **Issue**:  The approach to strategic issue management is still to be reviewed and formally signed off, with updated strategy, policy and guidance not yet completed.<br>Review of the documents in place, discussion with staff and our comparison with strategic risk management noted the following are not currently reflected in the strategic issue management approach:<br>- clearly defined roles and responsibilities are not set out within guidance documents, relevant Terms of Reference or delegation letters (or key staff job descriptions/role objectives)<br>- Reference to strategic issue management and the links to strategic risk management within the Risk Management Strategy (or separate Issue Management Strategy). | strategic issue management and, where appropriate, ensure strategies, guidance and processes are documented to support the agreed approach, with action taken to implement to ensure issues are effectively managed. | 🟥 | **Action:**<br>We will look to implement a proportionate issues management strategy.  This will be detailed within our Risk Management Strategy and covered within Risk Management Training.  Issues resolution activity will be managed within business as usual.<br>**Action Owner:**<br>Corporate Assurance and Risk Team Leader |  |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | - The process for identifying strategic issues, together with guidance on how to define / word them clearly and correctly, with a clear distinction between risks and issues made, and clearly setting out the different management processes.<br>- Method for recording, monitoring and tracking strategic issues, including the linked strategic risks.<br>- Process for reviewing responses to strategic issues, which, once in place, should include sufficient challenge and frequency of review of these actions to ensure that they are still appropriate.<br>- The route for closure for strategic issues where they have become eliminated.<br>- A lessons learned process to identify what caused strategic risks to materialise into strategic issues. | | 🟥 | | |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | **Risk:** An inability to effectively manage strategic issues leading to an inability to achieve strategic objectives**.** | | 🟥 | | |
| 6 | Training<br>**Issue**: Although Social Security Scotland staff have access to the same Risk Management training on Pathways as core Scottish Government staff, unlike for core Scottish Government staff, completion of this training is not mandatory. This includes those colleagues who have specific responsibilities in relation to risk management.<br>Social Security Scotland Pathways and Saltire information is focussed on general risk management, rather than strategic risk management and there is no specific training on strategic issue management. | Management should consider making risk management training mandatory for relevant roles to increase awareness in, and create a culture of, risk management.<br>Training should continue to be developed to include strategic risk and strategic issue management, with a log retained of who has received training. | M | **Response:**<br>Recommendation Accepted<br>**Action:**<br>We will review and enhance our risk management training available on Pathways to reflect the new Strategic Risks and strategy/framework.<br>Risk management is a shared responsibility and key behaviour for all civil servants. This is not unique to Social Security Scotland. There is a clear link here to objective setting, in line with general Scottish Government guidance. | October 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | Where bespoke training and workshops have been delivered by the Risk Team, a log has not been retained to evidence who was present at these sessions or who has completed what training on Pathways.<br>**Risk 1:** Insufficient and/or ineffective strategic risk management strategy, policy, guidance and training.<br>**Risk 2:** Insufficient and/or ineffective strategy, policy, guidance and training in relation to the management of issues. | | | We will detail issues management within the risk training and documentation as is proportionate.<br>**Action Owner:**<br>Risk and Assurance Team Leader | |
| 7 | Management Oversight<br>**Issue:** Although the Strategic Risk Register is presented to the Executive Team it is a 'below the line item', and we have not seen evidence to suggest any discussion or scrutiny at the meetings. | The Risk Team should continue liaison with the Executive Team, Chief Executive and Deputy Directors to agree a format of reporting which meets their needs. | **M** | **Response:**<br>Recommendation Accepted<br>**Action:**<br>Risk Management reporting to the Executive Team and other appropriate governance forums is in development. | August 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | Regular reporting (i.e. to the Executive Team, Chief Executive and Deputy Directors) is not yet in place as the format and content of reporting has yet to be agreed.<br>Whilst the Risk Review Group Terms of Reference states "Where permanent members are unavailable they will provide a deputy with the appropriate authority to make strategic decisions", this was not always happening in practice resulting in the cancelation of the group (December 2023) with potentially strategic risks not being considered for addition to the Strategic Risk Register.<br>Additionally, there does not appear to be any formal arrangements for oversight and scrutiny of issue management activities as it is not included in the Terms of Reference for the Audit and Assurance Committee or Executive | Management should ensure that sufficient time is allocated for discussion, to allow sufficient oversight and scrutiny of strategic risk management.<br>Reporting arrangements for strategic issue management should be agreed and, as above, regular reporting and time for discussion should take place to allow sufficient oversight and scrutiny | 🟨 | Work on this will be completed by August 2024.<br>Risk Review is a governance group that reports directly to Executive Team, we will look to make this link and the reporting arrangements more explicit.<br>Issues management is already discussed at our governance groups as this is managed in business as usual. However we will reflect the retrospective investigatory work of the risk management team within the Risk Review Group Terms of Reference and strategy documents.<br>**Action Owner:**<br>Risk and Assurance Team Leader | July 2024<br>August 2024 |

| No. | Issue & Risk | Recommendation | Priority | Management Response & Action Owner | Action Date |
|---|---|---|---|---|---|
| | Team, nor have we seen any evidence of discussion at these forums.<br>**Risk 1:** Insufficient and/or ineffective arrangements for oversight and scrutiny of risk management activities, identified risks and mitigating actions and controls.<br>**Risk 2:** Insufficient and/or ineffective arrangements for oversight and scrutiny of issue management activities. | of strategic issue management.<br>Management should also review the circumstances surrounding the late cancelation of the December 2023 Risk Review Group, to identify if any lessons can be learned to ensure that future meetings go ahead with the required attendees. | 🟨 | | |

## 3. Findings, Good Practice and Improvement Opportunities

### 3.1. Good Practice

Roles and Responsibilities

3.1.1. The roles and responsibilities for risk management within Social Security Scotland are captured in the draft Risk and Issue Management Framework, in delegation letters for Deputy Directors and in the draft Risk Handbook for the Risk Team. The Terms of Reference for the Risk Review Group and Audit and Assurance Committee clearly outline the risk management roles and responsibilities of both.

3.1.2. A risk management update is a standard agenda item at each Audit and Assurance Committee and risk management is covered in the Audit and Assurance Committee annual report.

3.1.3. The Risk Review Group is chaired by a Deputy Director from Social Security Scotland, providing a direct link between the group and the Executive Team. Our review of the Risk Review Group minutes from the August meeting confirmed that feedback from the Executive Team was provided.

Stakeholder Engagement

3.1.4. The chair of the Audit and Assurance Committee attended a session of the Risk Review Group to support the development of the new approach to strategic risk management and the new strategic risk register.

3.1.5. The Risk Team are actively improving risk management arrangements and practices across the organisation and provide a collaborative and supportive approach to the rest of the organisation. (e.g. attendance at divisional meetings, engagement with the Executive Team, tailored training and support, etc.).

3.1.6. There is representation from Social Security Scotland on Social Security Programme's Risk Review Panel and from Social Security Programme on Social Security Scotland's Risk Review Group in recognition of their respective impacts. In addition, there are monthly meetings between Social Security Scotland and Social Security Programme's risk teams.

3.1.7. The Senior Leader Brief is used as a communication channel allowing for information sharing of updates to risk management arrangements and dissemination to other staff as appropriate.

3.1.8. Through fieldwork discussions we noted positive feedback on the updated Strategic Risk Register from senior leaders across the organisation, as well as from the Non-Executive Directors at the November 2023 Audit and Assurance Committee meeting.

## 3.2. Improvement Opportunities

Roles and Responsibilities

3.2.1. Only limited information on the Risk Team is available on Saltire, which could lead to a risk of poor understanding of risk management and processes within Social Security Scotland. Information could be expanded upon to set out the roles and responsibilities of the team, how it is there to support the organisation, as well as containing guidance (once finalised) and links to training on Pathways. **Recommendation 1**

3.2.2. The Terms of Reference for Social Security Scotland's Executive Team sets out its responsibility for strategic risk management and the reporting of same into the Executive Team. However, it is still in a draft form and should therefore be finalised and signed off to ensure the group is clear on its roles and responsibilities. **Recommendation 2**

3.2.3. The Risk Review Group Terms of Reference contains references to the Agency Leadership Team which is no longer in place, this is also depicted in a diagram which shows the previous governance structure of Social Security Scotland(similar diagrams are also in the Risk Handbook and Risk Framework). **Recommendation 2**

Documented Processes

3.2.4. The Risk and Issue Management Framework, Risk Strategy and Risk Team Handbook were under review during our fieldwork. These should be completed and updated to reflect current and future arrangements and these should be shared with appropriate stakeholders. **Recommendation 3**

3.2.5. While we are aware that there is representation from Social Security Scotland on Social Security Programme's Risk Review Panel (and vice versa), with many of the strategic risks and issues shared by both parties, guidance should explain how to cross reference risks and clarify arrangements for information sharing and interaction for both strategic and divisional risks. **Recommendation 3**

3.2.6. While it is good practice that risks on the Strategic Risk Register are being updated to contain links to relevant Divisional risks, the process for closure/removal of Divisional risks from the Strategic Risk Register is still to be set out in guidance. **Recommendation 3**

3.2.7. The Risk Review Group has a delegated responsibility for scrutiny and challenge of strategic risk management which includes review and scrutiny of mitigating actions and controls. We however note that guidance for what good looks like wasn't in place to allow for evaluation of compliance with Social Security Scotland's risk management requirements and to allow for sufficient challenge where mitigating actions and controls are not sufficient. Guidance should be developed to highlight that mitigating controls should clearly set out the key controls and include timescales i.e. when the target risk score is anticipated to be achieved. **Recommendation 3**

3.2.8. Neither the Risk and Issue Management Framework nor the Risk Strategy detail how the output of the risk management process will inform the business planning or decision-making processes. We note that strategic risks have recently been linked to strategic objectives and all papers going to the Executive Team for decision require to be linked to a strategic risk(s), further strengthening and embedding the risk management process in business planning and decision making, however this process has not been documented to ensure risk management is embedded in all business planning and decision making activities. **Recommendation 3**

Risk Management Approach

3.2.9. Risk appetite and tolerance setting are important elements of risk management and are used to inform decision making, however our review found that guidance and approach to establishing risk appetite and tolerance levels has not been captured and risk appetite and tolerance levels have not been set. **Recommendation 4**

3.2.10. Our review found that Social Security Scotland instructs staff to follow risk management best practice and follow the Scottish Government risk management guidance for identifying, recording and managing risks. As part of this review we also noted that, while the strategic risk register mainly follows risk management best practice, not all risks are written in line with risk management guidance, with some being worded more like statements (i.e. CR-005, CR-008 and CR-011). It is important that a consistent approach is implemented for articulating strategic risks to ensure these can be understood and the risk facing Social Security Scotland is known, which allows for relevant controls and mitigations to be identified and implemented. **Recommendation 4**

3.2.11. Whilst we recognise that work is still ongoing to fully populate the strategic risk register, our review of mitigating actions for strategic risks and of current controls and mitigations for divisional risks found that these were worded inconsistently and the field that outlines ‘planned action to achieve target risk score’ was not completed for all risks. **Recommendation 4**

Some of the detail we noted from our review includes:

1) Mitigating controls for risks 3 and 9 did not contain sufficient detail and not all divisional risks linked to these strategic risks contained a mitigating action.

2) The mitigating control field for the divisional risk linked to strategic risk 8 stated: “CDO taken actions to address reference attached email”. However,

the email was not attached and no detail of what was in the email was captured in the register.

3) Planned action to achieve target risk score was not completed for Risk 6.

Issue Management Approach

3.2.12. Whilst the Risk and Issue Management Framework sets out the roles, responsibilities and reporting lines for strategic risk management, this is not included for strategic issue management. In addition, the Terms of Reference for the Risk Review Group sets out escalations and exceptions in relation to Strategic Issues, however it does not set out any responsibilities in relation to the Strategic Issues Log (which it does for the Strategic Risk Register). **Recommendation 5**

3.2.13. Updated strategy, policy and guidance in relation to strategic issue management are not yet in place due to the recent change in process for managing strategic risks being the focus for improvement to date. Whilst the draft Risk and Issue Management Framework contains a section outlining the Issue Management process, including strategic issues, there is no reference to issue management within the Risk Management Strategy (or a separate Issue Management Strategy). **Recommendation 5**

3.2.14. The process for identifying issues, at both Divisional and Strategic levels, needs to be clarified and communicated to staff together with guidance on how to define/word strategic issues clearly and correctly, with a clear distinction between risks and issues made. The draft framework states that "if the issue requires a business continuity or incident management response, it will be managed under those process", however does not distinguish between these processes to avoid confusion and staff following the inappropriate escalation route. **Recommendation 5**

3.2.15. The draft framework states that strategic issues require immediate action plans that must be established and tracked. Our review found that the strategic risk register is only just being developed to include linkages to strategic issues and that the Strategic Issues Log is not being regularly updated or discussed (see 3.2.23). Again, the approach to issue management needs to be reviewed and agreed by management before implementation and this has not been done. **Recommendation 5**

3.2.16. We found that a process for reviewing responses to strategic issues had not yet been agreed, documented, or communicated to staff. Management should ensure that they have an effective mechanism for identifying and recording appropriate responses, ensuring these responses are taken and monitoring that they have the desired impact on the issue. As part of this there should be sufficient challenge and frequency of review of these actions to ensure that they are still appropriate and effective in managing the identified issues. **Recommendation 5**

3.2.17. The route for closure or de-escalation of strategic issues once they are resolved was not clarified, documented or communicated to staff to ensure consistency in approach. Management should also consider introducing a lessons learned process to identify what caused strategic risks to materialise into strategic issues. **Recommendation 5**

### Training

3.2.18. Social Security Scotland staff have access to the same Risk Management training on Pathways as core Scottish Government staff, however, unlike for core Scottish Government staff none of this is mandatory. We would recommend consideration is given to making risk management mandatory learning for appropriate roles to increase awareness in, and create a culture of, risk management for those with responsibility for risk management activities across the organisation. **Recommendation 6**

3.2.19. Social Security Scotland Pathways and Saltire information is focussed on risk management at a divisional level, rather than Social Security Scotland's approach to strategic risk management. While we were informed that more advanced courses covering strategic risk management are going to be developed, these were not in place at the time of our fieldwork.

3.2.20. In addition, there is no specific training on strategic issue management, although we recognise that there are elements of issue management within the existing risk management training and that the strategic issue management process has still to be developed. We were advised that specific training is planned for strategic issue management once this has happened. **Recommendation 6**.

3.2.21. While bespoke training and workshops are delivered by the Risk Team as and when required (e.g. risk awareness sessions have been developed and delivered to the Risk Review group and divisions), a log has not been retained to evidence who was present at these sessions or who has completed what training on Pathways. **Recommendation 6**

Management Oversight

3.2.22. The strategic risk register is a 'Below the Line' item at each Executive Team meeting. Having reviewed meeting minutes we did not find evidence to suggest that the strategic risk register was discussed. In addition, quarterly reporting to the Executive Team has not yet been established. However, this has already been recognised as a gap and we were advised that discussions are taking place to agree the format and content of reporting to the Executive Team. Furthermore, the plan is that the Risk Review Group will agree and issue appropriate reports to the Chief Executive and Deputy Directors as and when appropriate, but at the time of our fieldwork, this wasn't in place yet. **Recommendation 7**

3.2.23. There does not appear to be any formal arrangements for oversight and scrutiny of issue management activities as it is not included in the Terms of Reference for the Audit and Assurance Committee or Executive Team, nor have we seen any evidence of discussion at these forums. **Recommendation 7**

3.2.24. The Terms of Reference for the Risk Review Group states that "Where permanent members are unavailable they will provide a deputy with the appropriate authority to make strategic decisions" our review found that this wasn't always happening in practice. Whilst the October meeting we observed was well attended, at the December Risk Review Group (moved from November due to annual leave) only six of the 19 permanent members of the group joined the call, which resulted in the meeting being called off as quorum (9) wasn’t met. Due to this meeting not going ahead, three risks that were due to be added to the Strategic Risk Register have been awaiting review and agreement by the Group since October 2023. The next meeting is scheduled for the end of January, due to peak leave at the end of December.  This is poor practice as this is almost a three-month period where mitigating controls and action plans for strategic risks that impact the achievement of strategic Social Security Scotland objectives have not been reviewed, scrutinised, and challenged as delegated by the Chief Executive. **Recommendation 7**

# Annex A Definition of Assurance and Recommendation Categories

## Assurance Levels

| | |
|---|---|
| **Substantial Assurance**<br>**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**<br>**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**<br>**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**<br>**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

# Directorate for Internal Audit and Assurance

# Internal Audit Terms of Reference

# Social Security Scotland 2023-24

# Risk Management

Directorate for Internal Audit and Assurance

**Issue Date**: 5-10-2023

## Key Audit Contacts

| | |
|---|---|
| **Audit Year:** | 2023-24 |
| **Client Accountable Officer:** | David Wallace, Chief Executive |
| **Deputy Director** | Ally MacPhail, Deputy Director, Organisational Strategy and Performance |
| **Client Audit Contact(s):** | James Wallace, Deputy Director Finance and Corporate Services<br>Head of Strategy and Corporate Support<br>Risk and Assurance Team Leader<br>Risk Team Manager<br>Deputy Programme Manager, Social Security Directorate<br>PMO Risk, Issue and Measurable Improvements Manager, Social Security Directorate |
| **Senior Internal Audit Manager:** | [Redacted] |
| **Internal Audit Manager:** | [Redacted] |
| **Internal Auditor(s):** | [Redacted] |

## Estimated Reporting Timescale

| | |
|---|---|
| **Fieldwork Starts:** | 9th October 2023 |
| **Fieldwork Ends:** | 10th November 2023 |
| **Draft Report Issued:** | 24th November 2023 |
| **Final Report Issued:** | 15th December 2023 |
| **Estimated Resource Days:** | 30 Days |

## 1. Introduction

1.1. This internal audit review forms parts of our planned audit coverage agreed by the Accountable Officer and noted by the Audit and Assurance Committee on 21st March 2023.

1.2. Managing risk effectively is important to ensure Social Security Scotland can achieve its strategic objectives, make informed decisions and protect the interests of its stakeholders. As such it is essential that Social Security Scotland have in place effective arrangements for risk management and the identification, assessment and control of risks.

1.3. Risk Management arrangements were previously reviewed by Internal Audit in 2019/20. Since then Social Security Scotland has continued to grow and mature. Recent work has been undertaken by the organisation to improve the arrangements for strategic risk management.

1.4. This review will focus on the risk management arrangements which have developed in Social Security Scotland since our previous review and assess the extent to which strategic risk management has become embedded in all activities such as business planning and decision making. The review will also consider the arrangements for the management of issues, a threat which has been realised

1.5. We met with Laura Smith, Risk and Assurance Team Leader and Simon Mitchell, Risk Team Manager, on 22nd August 2023 to discuss relevant risks and scope of this review. Our key risks below have been developed through this discussion and our knowledge of Risk Management and Social Security Scotland.

## 2. Scope

2.1. To evaluate and report on Social Security Scotland’s Strategic Risk Management arrangements, the controls in place to identify, record, manage/mitigate and report on risks facing the organisation along with the arrangements for management of issues.

### 2.2. Remit Item 1 – Risk Management Arrangements

An assessment of the effectiveness of the arrangements established for strategic risk management including the identification and assessment of strategic risks and their mitigating controls, mechanisms for recording and reporting on strategic risks and an assessment of the arrangements for monitoring and scrutinising the risk management activities of Social Security Scotland.

Key Risks:

- Poor understanding and awareness of risk within Social Security Scotland leading to a failure to adequately embed the appropriate risk management practices.
- An inability to effectively manage strategic risks leading to an inability to achieve strategic objectives due to:
  - Appropriate roles and responsibilities, lines of reporting and accountability for strategic risk management not been established and embedded across the organisation.
  - Insufficient and/or ineffective strategic risk management strategy, policy, guidance and training.
  - Insufficient and/or ineffective arrangements for oversight and scrutiny of risk management activities, identified risks and mitigating actions and controls.
  - Inappropriate approach and methodologies for identifying, recording and managing risks.
  - Lack of review of the effectiveness of identified mitigating actions.
  - Ineffective arrangements for escalation of divisional and/or Social Security Directorate risks which may impact Social Security Scotland's strategic objectives.
  - Non-compliance with established strategic risk management processes.
- Risk management output not being utilised effectively to ensure decisions are risk based and risk management is embedded in business planning and decision making leading to inappropriate decisions being made and an inability to take advantage of opportunities arising.

### 2.3. Remit Item 2 – Strategic Issue Management

An assessment of the effectiveness of the arrangements established for the management of strategic issues (strategic risks which have been realised) including the identification and assessment, the mechanisms for recording and reporting and the established processes for identifying and implementing remedial actions.

Key Risks:

- An inability to effectively manage strategic issues leading to an inability to achieve strategic objectives due to:
    - Appropriate roles and responsibilities, lines of reporting and accountability for strategic issue management not been established and embedded across the organisation.
    - Insufficient and/or ineffective strategy, policy, guidance and training in relation to the management of issues.
    - Insufficient and/or ineffective arrangements for oversight and scrutiny of issue management activities.
    - Inappropriate approach and methodologies for identifying, recording and managing issues.
    - Lack of review of the implementation and effectiveness of identified remedial actions.
    - Ineffective arrangements for escalation of divisional and/or Social Security Directorate issues which may impact Social Security Scotland's strategic objectives.
    - Non-compliance with established strategic issue management processes.

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