## Audit and Assurance Committee

| | |
|---|---|
| Date of Meeting | Tuesday 13 November 2018 |
| Subject | Risk Management Strategy |
| Agenda No. | 4 |
| Paper No. | 1.2 |
| Prepared By | [redacted] |
| Purpose | Decide |

## 1. Background

1.1. The Audit and Assurance Committee is invited to consider, discuss and, if content, agree Social Security Scotland's ("the Agency's") risk management strategy for roll-out across the Agency.

## 2. Key Points

2.1. The document sets out the approach to managing risk within the Agency. It describes:

- the places where business unit-level risks, project risks and strategic risks are recorded, and the people responsible for ensuring that these are recorded appropriately,
- the process used to record and assess the probability and impact of risks,
- the processes by which risks are escalated,
- the escalation routes when risks require action or decisions, and
- [redacted]

## 3. Conclusions

3.1. The Audit and Assurance Committee is invited to consider the attached document and to indicate if it is content for the strategy to be rolled-out across the Agency, or if it wishes the strategy to be changed in any way. Subject to the Audit and Assurance Committee being content, the strategy will, hereafter, be forwarded to the Executive Advisory Body for their views before being submitted to the Chief Executive for final approval.

GOVERNANCE CHECKLIST

| Strategic consideration | Impact |
|---|---|
| Environment | The strategy does not have any environmental implications beyond the fact that environmental risk will be a type of risk which will be managed via the strategy |
| Governance | The strategy has been agreed by the Head of Governance and Strategy, for her interests. It operates within the Agency's existing governance framework – for agreement by the Chief Executive after consideration by Audit and Assurance Committee. |
| Data | The strategy does not have any data implications beyond the fact that there are various 'data risks' which will be managed via the strategy |
| Finance | The strategy does not have any financial implications beyond the fact that financial risk will be a type of risk which will be managed via the strategy |
| Staff | The strategy has implications for staff training which will be managed, at least initially, via the currently agreed resource envelope for the Governance and Strategy Unit. However, the staffing impacts of the strategy will need to be reviewed in due course. |
| Equalities | The strategy does not have any equalities implications |
| Estates | The strategy does not have any implications for the Agency estate beyond the fact that 'estates risk' will be a type of risk which will be managed via the strategy |
| Communications and Presentation | A communications plan, to explain and support the roll-out of the strategy will be developed in due course. |

# Social Security Scotland:

# Risk Management Strategy (incorporating Risks & Issues)

Document History

| Date | Updated by | Version | Reason for change |
|---|---|---|---|
| 26/05/17 | AP | 0.7 [redacted] | Updated version for peer review |
| 12/10/18 | CB | 1.0 | Updated version for SSS use. |
| 26/10/2018 | CB | 1.1 | Updated after peer review |
| 2/11/2018 | CB | 1.2 | Updated for issue to SLT |
| 6/11/2018 | CB | 1.3 | Updated for issue to AAC |

Table of Contents:

## 1. Risk Management Strategy

1.1. This document sets out the approach to managing risk within Social Security Scotland ("the Agency"). It describes:

- the places where business unit-level risks, project risks and strategic risks are recorded, and the people responsible for ensuring that these are recorded appropriately,
- the process used to record and assess the probability and impact of risks,
- the processes by which risks and issues are escalated,
- the escalation routes when risks and issues require action or decisions, and
- [redacted]

## 2. Recording Risks

2.1. There are three categories or levels of risk: 'business unit risks', 'risks' and 'strategic risks':-

- **business unit risks**[1] are recorded in concerns logs, held and maintained at business unit level[2],
- **project risks** are recorded in project risk registers by projects reporting into the Transformation and Change Board (the "Change Board") and in the Change Board Risk Register.
- **strategic risks** are collated by the Agency's risk management function, which is within the Governance and Strategy Unit, and are used to populate and maintain the Strategic Risk Register ("SRR") which is held and maintained at Agency Chief Executive/Senior Leadership Team level.
- the format of the SRR will reflect the Scottish Government Risk Register Template[3], which is based on an internationally recognised risk register model.

2.2. The Agency's Senior Leadership Team ("SLT") (with the support of the Agency's risk management function) are responsible for ensuring that:-

[1] The reason for recording 'business unit risks' in 'concerns logs' (which will be used to capture business unit issues, as well as risks) rather than risk logs is to ensure that the process by which risks and issues are identified and captured at the operational level can be made as simple as possible and can be carried out without the need for in-depth training

[2] "Agency Business Units" means any team with a team-leader who reports directly to a member of the Agency's Senior Leadership Team).

[3] See: http://saltire/_layouts/15/download.aspx?SourceUrl=%2FDocuments%2FFinance%2520documents%2FCorporate_risk_register_template.xlsm&FldUrl=&Source=http%3A%2F%2Fsaltire%2Fmy-workplace%2Ffinance%2FPages%2FRisk-management.aspx%3Fpageid%3De4005ede-ae4f-4719-8a91-e9e362840c6d

- concerns logs are in place in each business unit,
- business unit risks are captured in concerns logs and interrogated at business unit level,
- concerns leads are identified, appropriate controls are in place, actions required to mitigate are taken and produce the required outcomes, and
- concerns logs are updated as required and individual business units report to the Agency's risk management function, to enable the effective maintenance of the SRR.

2.3. The Agency's risk management function will work with owners in individual business units to assess business unit risks and countermeasures.

2.4. The Agency's Transformation and Change Team is responsible for ensuring that:-

- project risk registers are in place for all projects reporting in to the Change Board,
- risks are captured in project risk registers and, where appropriate, in the Change Board Risk Register and are interrogated at the appropriate level,
- risk owners are identified, appropriate controls are in place, actions required to mitigate are taken and produce the required outcomes, and
- risk registers are updated as required and individual projects report into the Change Board, to enable the effective management of risk at Change Board level.

2.5. The Agency's risk management function is responsible for ensuring that:-

- risk management culture is deeply embedded across the Agency, all Agency staff understand the importance of risk management and have access to the expertise, methodologies and tools to effectively manage risk in their respective, local areas,
- the SRR is in place and fit for purpose, strategic risks are captured on the basis of evidence submitted via individual business units' concerns logs,
- the Agency's Transformation and Change Team is given the necessary advice and support, in relation to the escalation of Change Board risks to the SRR,
- risk action leads are agreed for each strategic risk, strategic risks are interrogated and challenged, appropriate controls are in place, actions required to mitigate/manage are taken and produce the required outcomes,
- the SRR is updated as required, and
- the Agency reports on risk effectively.

2.6. [redacted]

2.7. The Agency's risk management function compiles and maintains the SRR. Changes to the SRR are reported to and considered by the Agency's Senior

Leadership Team ("SLT") and Chief Executive, the Agency's Audit and Assurance Committee ("AAC") and, thereafter (via the AAC's reports), the Agency's Executive Advisory Body ("EAB"). The Agency's Chief Executive, in their role as Accountable Officer is the owner of the SRR.

2.8. For each meeting of the AAC, the Agency's risk management function will provide a report designed to update members on the risk status changes since the last meeting and the Top 10 risks for the Agency. The Top 10 are typically defined as the current highest scoring risks. The templates on how these updates are presented may evolve over time.

2.9. Similar arrangements will exist at business unit level.

## 3. Assessing Strategic Risks

3.1. Strategic risks are assessed by following the standard SG approach to risk management, as set out in the Scottish Government's Risk Guide[4]. Unless specifically stated otherwise (e.g. concerns logs) – the document set, methodologies, tools etc. used in assessing Agency risk will be as per the Risk Guide.

3.2. The probability of the risk occurring is rated 1-5, with 5 being very high and 1 being rare. The impact of the risk if it occurs is rated separately, with 50 being a very high impact and 1 being a negligible impact. These scores are multiplied together to give a risk score. Actions to mitigate risks can either reduce the likelihood of the risk occurring, or the impact if the risk occurs; this is shown in a reduction to either the likelihood rating or the impact rating and results in a new risk score based on action being taken.

## 4. Managing Strategic Risks

4.1. The Agency will manage strategic risks in order to keep them within the limits of its 'risk appetite'[5]. The Agency's risk management function will carry out an initial 'baselining' exercise, in order to establish the Agency's risk appetite for agreement with the AAC, and the CE, as Accountable Officer.

[4] See: http://saltire/_layouts/15/download.aspx?SourceUrl=%2FDocuments%2FFinance%2520documents%2FRisk_management_guide.pdf&FldUrl=&Source=http%3A%2F%2Fsaltire%2Fmy-workplace%2Ffinance%2FPages%2FRisk-management.aspx%3Fpageid%3De4005ede-ae4f-4719-8a91-e9e362840c6d

[5] Risk appetite means the levels and types of risk the Agency is prepared to accept (and not accept) in progressing towards the strategic objectives set out in its Corporate Plan.

4.2. Once agreed, the Agency's risk appetite sets the risk boundary for the Agency and provides the Agency's risk management function, the AAC, EAB, CE and all staff involved in managing agency risk with a clear understanding of which risks (and mitigation/management activity) to prioritise.

4.3. The Agency's risk management function will work with the AAC to establish the Agency's risk appetite, for ratification by the CE. When setting the Agency's risk appetite, the Agency's risk management function will consider:

- impact on individuals of services not being delivered to the required standards,
- readiness and capacity for the Agency to take on change,
- reputational impact of failure,
- the ability of the Agency to deliver at the pace required, and
- the risk management structures in place.

4.4. The Agency's risk appetite (along with the rest of this strategy) will be reviewed periodically.

4.5. Managing the Agency's strategic risks, and keeping them within the boundaries of the Agency's risk appetite, means managing a matrix of risks at three levels - the Agency's strategic risk level, the Agency's Transformation and Change Board level and the Agency's individual business unit level.

4.6.The Agency's risk management function will hold monthly meetings with the risk action leads shown in the SRR where risks will be reviewed, scoring agreed and any updates to mitigation and actions will be recorded. Risks may also be revised on a more immediate basis when required. The updates and any proposed changes to scoring are recorded in the SRR register for the attention of the AAC.

4.7. At each AAC meeting, the Agency's risk management function will provide a detailed update and draw the Committee's attention to:

- any new strategic risks which have been identified since the last Committee meeting,
- any mitigating actions which have occurred or should have occurred since the last Committee meeting, and
- any proposed changes to risk scores since the last Committee meeting.

4.8. The Change Board will be responsible for governing, monitoring and supporting the progress of projects across the Agency, particularly those that have an significant organisational impact and those that are part of the wider Social Security Programme. The Change Board will also oversee management of the risks relating to the projects reporting into the Change Board.

4.9.The Agency's risk management function will hold monthly meetings with the Change Board team, to agree whether Change Board risks should be escalated to the SRR and, if so, to agree scoring and record mitigating actions and controls. Thereafter, the Change Board risks which have been escalated will be reviewed in the same way as all other risks in the SRR.

4.10. [redacted]

4.11. The Agency's SLT is responsible for arrangements to manage concerns logs at individual business unit level. It is suggested, though it is not a requirement, that unit heads should meet regularly with the Concerns Lead (or leads) and risk action leads within their respective units. (A Concerns Lead and a Risk Action Lead may, sometimes, be the same person, if a risk has been escalated to the SRR and it has been agreed that the relevant individual will be responsible for ensuring that the necessary strategic action is taken and reported on.)

4.12. Individual business units' concerns logs should identify the top ten risks to each business unit as well as any new risks that have been raised. Individual business units' risks will be escalated to the SRR - with the agreement of the Agency's risk management function and after appropriate interrogation and challenge - and will be then be managed at Agency level.

4.13. The Agency's risk management function will hold regular meetings with individual business units' concerns leads, to agree whether risks should be escalated to the SRR and, if so, to agree scoring and record mitigating actions and controls. Thereafter, the individual business units' risks, which have been escalated to become strategic risks, will be reviewed in the same way as all other risks in the SRR.

4.14. The Agency's risk management function will record any further mitigating action proposed by the AAC - and/or any change to strategic risk ratings as a result of the AAC's consideration - which will then be submitted to the CE, in their role as Accountable Officer, for agreement.

**5.** [redacted]

5.1. [redacted]

5.2. [redacted]

5.3. [redacted]

5.4. [redacted]

5.5. [redacted]

[redacted]

5.6. [redacted]

[redacted]

5.7. [redacted]

[6] See: https://dgxmvz0tqkndr.cloudfront.net/production/images/general/3830_Social_Security_Scotland_Report_Online.pdf

[redacted]

5.8. [redacted]

5.9. [redacted]

5.10. [redacted]

5.11. [redacted]

5.12. [redacted]

## 6. Audit and Assurance Committee

6.1. The AAC will meet on a quarterly basis to review the SRR and provide the CE with the assurance that risks are being managed accordingly. The AAC members consist of non-executive members of the EAB, and independent external members). The AAC will be chaired by a non-executive member of the Executive Advisory Body or an independent member.

6.2. The Agency's risk management function is responsible for providing the AAC with sight of the SRR and any other required documentation ahead of each meeting. Any proposed changes to mitigation and actions are reviewed, any requests for changes to risk scoring are presented and agreed and any new strategic risks that are considered as an Agency risk are discussed and agreement reached. The reports of the AAC ultimately feed into the information the EAB receive on risk.

## 7. Business Unit Risks

7.1. Business units' risks will be recorded in the appropriate concerns log. The Unit Head is the owner of the Business Unit's concerns log (though it is expected that the Unit Head will delegate responsibility for maintaining and updating the concerns log to another member of their Unit – their Concerns Lead).

7.2. The Agency's risk management function will provide advice in relation to risks and countermeasures to each business unit.

7.3. Concerns Leads will capture new risks and countermeasures and update the concerns log accordingly, update the status of existing risks and countermeasures, review the concerns log on a monthly basis and report to the Agency's risk management function.

7.4. Concerns leads will also be responsible for ensuring that the originator of the risk (where this individual is not also the Concerns Lead) receive updates on their risk and the countermeasures put in place.

## 8. Template for Concerns Log

8.1. Individual business units' concerns logs will be as per the attached spread-sheet:-

Governance - Organisational Strat

## 9. Escalating Business Unit Risks

9.1. The Agency's risk management function will work with individual business units' concerns leads to identify business unit risks which require to be escalated to the SRR. New risks raised to the SRR will be discussed at the next meeting of the AAC. The Agency's risk management function will provide individual business units with guidance on the procedure for raising risks to the SRR.

## 10. Issue Management Strategy

10.1. This section outlines our approach to managing issues captured across the Agency.

10.2. Issues are events or conditions that have negative consequences for the Agency. It is usually assumed that issues are recoverable or that they can be mitigated in some way (though this may not always be the case). Issues differ from risks in that risks will not have occurred at the time at which they are identified.

10.3. For example, a lack of resource which may impact on the agency's ability to deliver a future service is a risk. A lack of resource, which has arisen because of illness, and which is currently impacting on agency services is an issue. The former needs to be managed, in order to prevent its materialising. The latter needs to be managed immediately, in order to prevent it having an impact or limit its impact.

10.4. Agency issues will, in many instances, derive from:-

- risks recorded in individual business units' concerns logs, which have materialised ('materialised' means that that the risk has occurred. When risks materialise, they will be closed as risks in all relevant logs/registers and captured as issues instead),
- issues recorded in individual business units' concerns logs, and
- strategic risks which have materialised.

10.5.However, issues can occur at any point and come from within or outside the Agency. Known issues which will have a cross-Agency impact will be documented in the Agency's Issues Log.

10.6. The Agency's risk management function is responsible for maintaining the Issues Log. This means capturing, examining and classifying Agency issues as they occur. will be as a result of interaction with SLT and individual Business Units.

10.7. Issues will be assessed by the Agency's risk management function. The Agency's risk management function will work with business units to agree the classification of issues and whether they can be managed at business unit level or if a specific issue requires notification to the SLT. If required, the Agency's risk management function will work with the business unit to draft the required notification. The SLT will then be notified of the issue, for assessment and proposed response. <u>All</u> amber/red issues will be notified to the SLT.

10.8. The RAG system will be used to categorise issues:

- **Red**: A significant issue which cannot be corrected by the Agency's risk management function working with the individual business unit. The issue is likely to have a serious impact on our ability to deliver and must be raised to the SLT/AAC/EAB/CE immediately.

- **Amber**: An issue which is likely to have a negative effect on the project or programme, but can be dealt with by the Agency's risk management function working with the individual business unit, without intervention from the SLT. It is imperative however that the SLT/AAC/EAB and CE are made aware of the issue via the Issues Log.

- **Green**: An issue which is considered to be minor and can be dealt with quickly and effectively by the Agency's risk management function working with the individual business unit, without having any impact on project delivery timescale or and/or costs.

10.9. The Agency's risk management function will assess progress made on outstanding issues at regular Issues Log meetings, to assess progress made on outstanding issues.

10.10. At these meetings the Issues Log will also be updated to reflect the impact an issue has had on previously identified strategic risks and/or to capture new risks created as a result of the issue.

10.11. SLT will discuss issues on a rolling monthly basis, issues will be updated in the Issues Log after each discussion and compared to the previous iteration of the SRR, to ensure that adequate progress towards resolution is being achieved.

10.12. All known possible courses of action will be considered with the most appropriate identified and responsibility for taking this forward assigned.

10.13. The SLT will review progress made on all red and amber issues and will propose corrective action where this is deemed necessary.

10.14. Irrespective of trend, any red or amber issue, which remains at this status for four consecutive weeks, will have a detailed update compiled outlining all corrective action being undertaken and planned and will be escalated to the AAC.

## 11. Roles and Responsibilities

11.1. The identification of risks and issues is the collective responsibility of everyone in the Agency, however specific responsibilities will sit with the following roles:

11.2. Social Security Scotland Chief Executive (the Accountable Officer):

- is the owner of the Social Security Scotland Risk Register.
- has ownership of strategic risks and issues and will ensure that these are managed effectively,
- authorises and initiates reviews of this strategy, and
- advises on overall organisational context and controls risks and issues which may impact on overall Agency level objectives.

11.3. Audit and Assurance Committee Chair:

- is responsible for scrutinising the adequacy of the Agency's processes for strategic risk management,
- chairs the AAC meetings, with support from the Agency's risk management function and Corporate Assurance Lead, and
- initiates reviews of this strategy.

11.4. Agency Risk Management Function:

- is responsible for ensuring that risks raised are properly recorded, and work with Risk Action Leads to initially assess the impact and likelihood of the risks, proposed mitigation and actions,
- is responsible for reviewing risks with Risk Action Leads in order to ensure progress with mitigating actions,
- is responsible for providing the agenda, risk summary and any other required documentation for the AAC,
- will hold monthly meetings with Risk Action Leads,
- ensures adherence to the Agency's risk management strategy,
- provides advice to wider team on management of risks and issues,
- maintains the Agency's SRR and Issues Log, and
- [redacted]

11.5. Individual Unit Heads:

- will support the work of risk action leads and concerns leads within their individual units,
- will facilitate robust consideration of all items which will impact on individual business units, and
- will ensure that risks, issues and countermeasures relating to individual business units are identified, captured, monitored, managed and reported effectively and in adherence to this strategy, and

11.6. Risk Action Leads:

- will agree (with the Agency's Risk Management Function) the controls required to mitigate/manage 'their' individual risk,
- will ensure that actions required to mitigate/manage are taken and progress is being made towards the required outcomes,
- will report on 'their' individual risks, to the Agency's Risk Management Function, and
- [redacted]

11.7. Individual Business Units' Concerns Leads

- will identify and capture new risks, issues and countermeasures and update their individual business units' concerns log accordingly,
- will update the status of existing risks, issues and countermeasures, review the concerns log on a monthly basis (with support from the Unit Head as/if required), and
- will report to the Agency's risk management function.

## 12. Reviewing the Strategy

12.1. The Agency's risk management function will review the risk management strategy (this document and any/all associated/dependant tools and document sets) after a period of no more than twelve months has passed since the strategy was agreed by the EAB and, thereafter, at intervals of the same period unless the EAB decides otherwise.

| Executive Advisory Body | |
|---|---|
| Date of Meeting | Tuesday 11 December 2018 |
| Subject | Risk Management Strategy |
| Agenda No. | 6 |
| Paper No. | 2.3 |
| Prepared By | [redacted] |
| Purpose | Decide |

## 1. Background

1.1. The Executive Advisory Body is invited to consider, discuss and, if content, agree Social Security Scotland's ("the Agency's") risk management strategy for roll-out across the Agency.

## 2. Key Points

2.1. The document sets out the approach to managing risk within the Agency. It describes:

- the places where business unit-level risks, project risks and strategic risks are recorded, and the people responsible for ensuring that these are recorded appropriately,
- the process used to record and assess the probability and impact of risks,
- the processes by which risks are escalated,
- the escalation routes when risks require action or decisions, and
- [redacted]

## 3. Conclusions

3.1. The Executive Advisory Body is invited to consider the attached document and to indicate if it is content for the strategy to be rolled-out across the Agency, or if it wishes the strategy to be changed in any way. Subject to the Executive Advisory Body being content, the strategy will, hereafter, be forwarded to the Chief Executive for final approval.

GOVERNANCE CHECKLIST

| Strategic consideration | Impact |
|---|---|
| Environment | The strategy does not have any environmental implications beyond the fact that environmental risk will be a type of risk which will be managed via the strategy |
| Governance | The strategy has been agreed by the Head of Governance and Strategy, for her interests. It operates within the Agency's existing governance framework – for agreement by the Chief Executive after consideration by Audit and Assurance Committee. |
| Data | The strategy does not have any data implications beyond the fact that there are various 'data risks' which will be managed via the strategy |
| Finance | The strategy does not have any financial implications beyond the fact that financial risk will be a type of risk which will be managed via the strategy |
| Staff | The strategy has implications for staff training which will be managed, at least initially, via the currently agreed resource envelope for the Governance and Strategy Unit. However, the staffing impacts of the strategy will need to be reviewed in due course. |
| Equalities | The strategy does not have any equalities implications |
| Estates | The strategy does not have any implications for the Agency estate beyond the fact that 'estates risk' will be a type of risk which will be managed via the strategy |
| Communications and Presentation | A communications plan, to explain and support the roll-out of the strategy will be developed in due course. |

# Social Security Scotland:

# Risk Management Strategy (incorporating Risks & Issues)

Document History

| Date | Updated by | Version | Reason for change |
|---|---|---|---|
| 26/05/17 | AP | 0.7 [redacted] | Updated version for peer review |
| 12/10/18 | CB | 1.0 | Updated version for SSS use. |
| 26/10/2018 | CB | 1.1 | Updated after peer review |
| 2/11/2018 | CB | 1.2 | Updated for issue to SLT |
| 6/11/2018 | CB | 1.3 | Updated for issue to AAC |
| 26/11/2018 | CB | 1.4 | Updated for issue to EAB |

**Table of Contents:**

## 1.Introduction

1.1. Social Security Scotland (hereafter also referred to as, "the Agency") exists for a purpose, which is defined in the Agency's interim Corporate Plan[1] as follows, "to administrate the Scottish social security system effectively, in accordance with the principles in the Act and Charter".

1.2. The delivery of this purpose, and the strategic objectives against which the Agency will measure its progress, is surrounded by uncertainty which poses threats to success.

1.3. Risk is defined as this uncertainty of outcome. Risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks and then responding to them.

1.4. The resources available to the Agency for managing risk are finite and so the aim is to achieve an optimum response to risk, prioritised in accordance with an evaluation of the risks.

1.5.Risk is unavoidable, and every organisation needs to take action to manage risk in a way which it can justify to a level which is tolerable. The amount of risk which is judged to be tolerable and justifiable is the "risk appetite".

1.6. Effective risk management needs to give full consideration to the context in which the Agency functions and to the risk priorities of partner organisations.

1.7. [redacted]

1.8.The management of risk at business unit, project and strategic levels needs to be integrated so that the levels of activity support each other. In this way the risk management strategy of the Agency can be led from the top and embedded in the normal working routines and activities of the organisation.

1.9.All staff should be aware of the relevance of risk to the achievement of their objectives and this strategy assumes that, upon its ratification, the appropriate level of training to support Agency staff in the management of risk will be made available.

[1] See: https://dgxmvz0tqkndr.cloudfront.net/production/images/general/3830_Social_Security_Scotland_Report_Online.pdf

## 2.Risk Management Strategy

2.1. The application of this risk management strategy will enable Social Security Scotland to obtain, maintain and respond to a changing risk appetite.

2.2.The active, on-going commitment and full support of the Social Security Scotland Executive Advisory Body ("the EAB") through the work of the Audit and Assurance Committee ("the AAC") and Social Security Scotland Senior Leadership Team ("the SLT") is an essential part of this strategy.

2.3.The Chief Executive and SLT will ensure that effective mechanisms are in place for assessing, monitoring and responding to any risks arising, whilst the EAB retain ultimate responsibility for overseeing the strategy.

2.4.This strategy sets out the approach to managing risk within Social Security Scotland ("the Agency"). It describes:

- the places where business unit-level risks, project risks and strategic risks are recorded, and the people responsible for ensuring that these are recorded appropriately,
- the process used to record and assess the probability and impact of risks,
- the processes by which risks and issues are escalated,
- the escalation routes when risks and issues require action or decisions, and
- [redacted]

2.5. Annex A sets out the key roles and responsibilities in relation to the delivery of this strategy.

## 3. Recording Risks

3.1. There are three categories or levels of risk: 'business unit risks', 'risks' and 'strategic risks':-

- **business unit risks**[2] are recorded in concerns logs, held and maintained at business unit level[3],
- **project risks** are recorded in project risk registers by projects reporting into the Transformation and Change Board (the "Change Board") and in the Change Board Risk Register.

[2] The reason for recording 'business unit risks' in 'concerns logs' (which will be used to capture business unit issues, as well as risks) rather than risk logs is to ensure that the process by which risks and issues are identified and captured at the operational level can be made as simple as possible and can be carried out without the need for in-depth training

[3] "Agency Business Units" means any team with a team-leader who reports directly to a member of the Agency's Senior Leadership Team).

- **strategic risks** are collated by the Agency's risk management function, which is within the Governance and Strategy Unit, and are used to populate and maintain the Strategic Risk Register ("SRR") which is held and maintained at Agency Chief Executive/Senior Leadership Team level.
- the format of the SRR will reflect the Scottish Government Risk Register Template[4], which is based on an internationally recognised risk register model.

3.2. The Agency's SLT (with the support of the Agency's risk management function) are responsible for ensuring that:-

- concerns logs are in place in each business unit,
- business unit risks are captured in concerns logs and interrogated at business unit level,
- concerns leads are identified, appropriate controls are in place, actions required to mitigate are taken and produce the required outcomes, and
- concerns logs are updated as required and individual business units report to the Agency's risk management function, to enable the effective maintenance of the SRR.

3.3. The Agency's risk management function will work with owners in individual business units to assess business unit risks and countermeasures.

3.4.The Agency's Transformation and Change Team is responsible for ensuring that:-

- project risk registers are in place for all projects reporting in to the Change Board,
- risks are captured in project risk registers and, where appropriate, in the Change Board Risk Register and are interrogated at the appropriate level,
- risk owners are identified, appropriate controls are in place, actions required to mitigate are taken and produce the required outcomes, and
- risk registers are updated as required and individual projects report into the Change Board, to enable the effective management of risk at Change Board level.

3.5. The Agency's risk management function is responsible for ensuring that:-

- risk management culture is deeply embedded across the Agency, all Agency staff understand the importance of risk management and have access to the expertise, methodologies and tools to effectively manage risk in their respective, local areas,

[4] See: http://saltire/_layouts/15/download.aspx?SourceUrl=%2FDocuments%2FFinance%2520documents%2FCorporate_risk_register_template.xlsm&FldUrl=&Source=http%3A%2F%2Fsaltire%2Fmy-workplace%2Ffinance%2FPages%2FRisk-management.aspx%3Fpageid%3De4005ede-ae4f-4719-8a91-e9e362840c6d

- the SRR is in place and fit for purpose, strategic risks are captured on the basis of evidence submitted via individual business units' concerns logs,
- the Agency's Transformation and Change Team is given the necessary advice and support, in relation to the escalation of Change Board risks to the SRR,
- risk action leads are agreed for each strategic risk, strategic risks are interrogated and challenged, appropriate controls are in place, actions required to mitigate/manage are taken and produce the required outcomes,
- the SRR is updated as required, and
- the Agency reports on risk effectively.

3.6. [redacted]

3.7. The Agency's risk management function compiles and maintains the SRR. Changes to the SRR are reported to and considered by the Agency's Senior Leadership Team ("SLT") and Chief Executive, the Agency's Audit and Assurance Committee ("AAC") and, thereafter (via the AAC's reports), the Agency's Executive Advisory Body ("EAB"). The Agency's Chief Executive, in their role as Accountable Officer ("AO") is the owner of the SRR.

3.8.Similar arrangements will exist at business unit level.

## 4. Audit and Assurance Committee

4.1. The AAC will meet on a quarterly basis to review the SRR and provide the CE with the assurance that risks are being managed accordingly. (The AAC members consist of non-executive members of the EAB, and independent external members). The AAC will be chaired by a non-executive member of the Executive Advisory Body or an independent member.

4.2.The Agency's risk management function is responsible for providing the AAC with sight of the SRR and any other required documentation ahead of each meeting.

4.3. For each meeting of the AAC, the Agency's risk management function will provide a report designed to update members on the risk status changes since the last meeting, the top risks for the Agency and any other related matters which it believes should be brought to the AAC's attention. The templates on how these updates are presented may evolve over time.

4.4. 'Top' risks are typically defined as the current highest scoring risks but there is no fixed number of 'top' risks in which the AAC may have an interest.

4.5. The Agency's risk management function will exercise its discretion (in line with the overarching requirement, to support the AAC in the full and effective discharge of its responsibilities) when deciding on the number of 'top' risks to bring to the AAC's attention and on any related matters on which it provides reports.

4.6. Proposed changes to mitigation and actions in relation to the 'top' risks will be reviewed by the AAC, requests for changes to risk scoring will be presented and agreed and new strategic risks, that are considered to be Agency risks, will be discussed and agreement reached.

4.7.After each meeting of the AAC, the Agency's risk management function will provide the EAB with a report on the AAC's discussion of Agency risk at its last meeting.

4.8. Reports will provide sufficient information to deliver on the AAC's purpose, defined in its Terms of Reference ("ToR") as being, "to provide [the EAB] with support in their responsibilities for issues of risk, control and governance and associated assurance through a process of constructive challenge".

4.9. These reports will be separate to the AAC's formal report in writing to the EAB and AO after each of its meetings which, as also stated in the ToR may take the form of a copy of the minutes of the meeting of the AAC. The AAC's first report to the EAB will comprise a copy of this strategy.

## 5. Assessing Strategic Risks

5.1. Strategic risks are assessed by following the standard SG approach to risk management, as set out in the Scottish Government's Risk Guide[5]. Unless specifically stated otherwise (e.g. concerns logs) – the document set, methodologies, tools etc. used in assessing Agency risk will be as per the Risk Guide.

5.2. The probability of the risk occurring is rated 1-5, with 5 being very high and 1 being rare. The impact of the risk if it occurs is rated separately, with 50 being a very high impact and 1 being a negligible impact. These scores are multiplied together to give a risk score. Actions to mitigate risks can either reduce the likelihood of the risk occurring, or the impact if the risk occurs; this is shown in a reduction to either the likelihood rating or the impact rating and results in a new risk score based on action being taken.

[5] See: http://saltire/_layouts/15/download.aspx?SourceUrl=%2FDocuments%2FFinance%2520documents%2FRisk_management_guide.pdf&FldUrl=&Source=http%3A%2F%2Fsaltire%2Fmy-workplace%2Ffinance%2FPages%2FRisk-management.aspx%3Fpageid%3De4005ede-ae4f-4719-8a91-e9e362840c6d

## 6.Managing Strategic Risks

6.1. The Agency will manage strategic risks in order to keep them within the limits of its 'risk appetite'[6]. The Agency's risk management function will carry out an initial 'baselining' exercise, in order to establish the Agency's risk appetite for agreement with the AAC, the EAB and the CE, as Accountable Officer ("AO").

6.2. Once agreed, the Agency's risk appetite sets the risk boundary for the Agency and provides the Agency's risk management function, the AAC, EAB, CE and all staff involved in managing agency risk with a clear understanding of which risks (and mitigation/management activity) to prioritise.

6.3. The Agency's risk management function will work with the AAC to establish the Agency's risk appetite, for ratification by the EAB and CE, as AO. When setting the Agency's risk appetite, the Agency's risk management function will consider:

- impact on individuals of services not being delivered to the required standards,
- readiness and capacity for the Agency to take on change,
- reputational impact of failure,
- the ability of the Agency to deliver at the pace required, and
- the risk management structures in place.

6.4. The Agency's risk appetite (along with the rest of this strategy) will be reviewed periodically.

6.5. Managing the Agency's strategic risks, and keeping them within the boundaries of the Agency's risk appetite, means managing a matrix of risks at three levels - the Agency's strategic risk level, the Agency's Transformation and Change Board level and the Agency's individual business unit level.

6.6.The Agency's risk management function will hold monthly meetings with the risk action leads shown in the SRR where risks will be reviewed, scoring agreed and any updates to mitigation and actions will be recorded. Risks may also be revised on a more immediate basis when required. The updates and any proposed changes to scoring are recorded in the SRR register for the attention of the AAC.

6.7. At each AAC meeting, the Agency's risk management function will provide a detailed update and draw the Committee's attention to:

- any new strategic risks which have been identified since the last Committee meeting,

[6] Risk appetite means the levels and types of risk the Agency is prepared to accept (and not accept) in progressing towards the strategic objectives set out in its Corporate Plan.

- any mitigating actions which have occurred or should have occurred since the last Committee meeting, and
- any proposed changes to risk scores since the last Committee meeting.

6.8. The Change Board will be responsible for governing, monitoring and supporting the progress of projects across the Agency, particularly those that have a significant organisational impact and those that are part of the wider Social Security Programme. The Change Board will also oversee management of the risks relating to the projects reporting into the Change Board.

6.9.The Agency's risk management function will hold monthly meetings with the Change Board team, to agree whether Change Board risks should be escalated to the SRR and, if so, to agree scoring and record mitigating actions and controls. Thereafter, the Change Board risks which have been escalated will be reviewed in the same way as all other risks in the SRR.

6.10. [redacted]

6.11.The Agency's SLT is responsible for arrangements to manage concerns logs at individual business unit level. It is suggested, though it is not a requirement, that unit heads should meet regularly with the Concerns Lead (or leads) and risk action leads within their respective units. (A Concerns Lead and a Risk Action Lead may, sometimes, be the same person, if a risk has been escalated to the SRR and it has been agreed that the relevant individual will be responsible for ensuring that the necessary strategic action is taken and reported on.)

6.12. Individual business units' concerns logs should identify the top ten risks to each business unit as well as any new risks that have been raised. Individual business units' risks will be escalated to the SRR - with the agreement of the Agency's risk management function and after appropriate interrogation and challenge - and will be then be managed at Agency level.

6.13.The Agency's risk management function will hold regular meetings with individual business units' concerns leads, to agree whether risks should be escalated to the SRR and, if so, to agree scoring and record mitigating actions and controls. Thereafter, the individual business units' risks, which have been escalated to become strategic risks, will be reviewed in the same way as all other risks in the SRR.

6.14.The Agency's risk management function will record any further mitigating action proposed by the AAC - and/or any change to strategic risk ratings as a result of the AAC's consideration - which will then be submitted to the CE, in their role as Accountable Officer, for agreement.

**7.** [redacted]

[redacted]

7.2. [redacted]

7.3 [redacted]

7.4. [redacted]

7.5. [redacted]

[redacted]

7.6. [redacted]

[redacted]

7.7 [redacted]

[redacted]

7.8 [redacted]

7.9 [redacted]

7.10 [redacted]

7.11 [redacted]

7.12 [redacted]

7.13 [redacted]

## 8. Business Unit Risks

8.1. Business units' risks will be recorded in the appropriate concerns log. The Unit Head is the owner of the Business Unit's concerns log (though it is expected that the Unit Head will delegate responsibility for maintaining and updating the concerns log to another member of their Unit – their Concerns Lead).

8.2. The Agency's risk management function will provide advice in relation to risks and countermeasures to each business unit.

8.3. Concerns Leads will capture new risks and countermeasures and update the concerns log accordingly, update the status of existing risks and countermeasures, review the concerns log on a monthly basis and report to the Agency's risk management function.

8.4. Concerns leads will also be responsible for ensuring that the originator of the risk (where this individual is not also the Concerns Lead) receive updates on their risk and the countermeasures put in place.

## 9.Template for Concerns Log

9.1. Individual business units' concerns logs will be as per the attached spread-sheet:-

Governance - Organisational Strat

## 10.Escalating Business Unit Risks

10.1. The Agency's risk management function will work with individual business units' concerns leads to identify business unit risks which require to be escalated to the SRR. New risks raised to the SRR will be discussed at the next meeting of the AAC. The Agency's risk management function will provide individual business units with guidance on the procedure for raising risks to the SRR.

## 11. Issue Management Strategy

11.1. This section outlines our approach to managing issues captured across the Agency.

11.2. Issues are events or conditions that have negative consequences for the Agency. It is usually assumed that issues are recoverable or that they can be mitigated in some way (though this may not always be the case). Issues differ from risks in that risks will not have occurred at the time at which they are identified.

11.3. For example, a lack of resource which may impact on the agency's ability to deliver a future service is a risk. A lack of resource, which has arisen because of illness, and which is currently impacting on agency services is an issue. The former needs to be managed, in order to prevent its materialising. The latter needs to be managed immediately, in order to prevent it having an impact or limit its impact.

11.4. Agency issues will, in many instances, derive from:-

- risks recorded in individual business units' concerns logs, which have materialised ('materialised' means that that the risk has occurred. When risks materialise, they will be closed as risks in all relevant logs/registers and captured as issues instead),
- issues recorded in individual business units' concerns logs, and
- strategic risks which have materialised.

11.5. However, issues can occur at any point and come from within or outside the Agency. Known issues which have a cross-Agency impact will be documented in the Agency's Issues Log.

11.6. The Agency's risk management function is responsible for maintaining the Issues Log. This means capturing, examining and classifying Agency issues as they occur will be as a result of interaction with SLT and individual Business Units.

11.7. Issues will be assessed by the Agency's risk management function. The Agency's risk management function will work with business units to agree the classification of issues and whether they can be managed at business unit level or if a specific issue requires notification to the SLT. If required, the Agency's risk management function will work with the business unit to draft the required notification. The SLT will then be notified of the issue, for assessment and proposed response. **All** amber/red issues will be notified to the SLT.

11.8. The RAG system will be used to categorise issues:

- Red: A significant issue which cannot be corrected by the Agency's risk management function working with the individual business unit. The issue is likely to have a serious impact on our ability to deliver and must be raised to the SLT/AAC/EAB/CE immediately.

- Amber: An issue which is likely to have a negative effect on the project or programme, but can be dealt with by the Agency's risk management function working with the individual business unit, without intervention from the SLT. It is imperative however that the SLT/AAC/EAB and CE are made aware of the issue via the Issues Log.

- Green: An issue which is considered to be minor and can be dealt with quickly and effectively by the Agency's risk management function working with the individual business unit, without having any impact on project delivery timescale or and/or costs.

11.9. The Agency's risk management function will assess progress made on outstanding issues at regular Issues Log meetings, to assess progress made on outstanding issues.

11.10. At these meetings the Issues Log will also be updated to reflect the impact an issue has had on previously identified strategic risks and/or to capture new risks created as a result of the issue.

11.11. SLT will discuss issues on a rolling monthly basis, issues will be updated in the Issues Log after each discussion and compared to the previous iteration of the SRR, to ensure that adequate progress towards resolution is being achieved.

11.12. All known possible courses of action will be considered with the most appropriate identified and responsibility for taking this forward assigned.

11.13. The SLT will review progress made on all red and amber issues and will propose corrective action where this is deemed necessary.

11.14. Irrespective of trend, any red or amber issue, which remains at this status for four consecutive weeks, will have a detailed update compiled outlining all corrective action being undertaken and planned and will be escalated to the AAC.

## 12. Reviewing the Strategy

12.1.The Agency's risk management function will review the risk management strategy (this document and any/all associated/dependant tools and document sets) after a period of no more than twelve months has passed since the strategy was agreed by the EAB and, thereafter, at intervals of the same period unless the EAB decides otherwise.

## ANNEX A

### Key Roles and Responsibilities

1.1.The identification of risks and issues is the collective responsibility of everyone in the Agency, however specific responsibilities will sit with the following roles:

1.2. Social Security Scotland Chief Executive (the Accountable Officer):

- is the owner of the Social Security Scotland Risk Register.
- has ownership of strategic risks and issues and will ensure that these are managed effectively,
- authorises and initiates reviews of this strategy, and
- advises on overall organisational context and controls risks and issues which may impact on overall Agency level objectives.

1.3. Audit and Assurance Committee Chair:

- is responsible for scrutinising the adequacy of the Agency's processes for strategic risk management,
- chairs the AAC meetings, with support from the Agency's risk management function and Corporate Assurance Lead, and
- initiates reviews of this strategy.

1.4. Agency Risk Management Function:

- is responsible for ensuring that risks raised are properly recorded, and work with Risk Action Leads to initially assess the impact and likelihood of the risks, proposed mitigation and actions,
- is responsible for reviewing risks with Risk Action Leads in order to ensure progress with mitigating actions,
- is responsible for providing the agenda, risk summary and any other required documentation for the AAC,
- will hold monthly meetings with Risk Action Leads,
- ensures adherence to the Agency's risk management strategy,
- provides advice to wider team on management of risks and issues,
- maintains the Agency's SRR and Issues Log, and
- works with the Programme Risk Manager to implement any/all arrangements necessary to ensure effective working across Programme and Agency risk management structures.

1.5. Individual Unit Heads:

- will support the work of risk action leads and concerns leads within their individual units,
- will facilitate robust consideration of all items which will impact on individual business units, and

- will ensure that risks, issues and countermeasures relating to individual business units are identified, captured, monitored, managed and reported effectively and in adherence to this strategy, and

1.6. Risk Action Leads:

- will agree (with the Agency's Risk Management Function) the controls required to mitigate/manage 'their' individual risk,
- will ensure that actions required to mitigate/manage are taken and progress is being made towards the required outcomes,
- will report on 'their' individual risks, to the Agency's Risk Management Function, and
- communicate with their counterpart[s] in the Programme, in relation to their individual risks and update the documentation, as required, to account for any updates by the Programme.

1.7. Individual Business Units' Concerns Leads

- will identify and capture new risks, issues and countermeasures and update their individual business units' concerns log accordingly,
- will update the status of existing risks, issues and countermeasures, review the concerns log on a monthly basis (with support from the Unit Head as/if required), and
- will report to the Agency's risk management function.