Social Security Scotland
Tèarainteachd Shòisealta Alba

Social Security Scotland Risk Management Framework

Version 1.4

Sep 2021

Dignity,
fairness,
respect.

Introduction

This document sets out the risk management framework for Social Security Scotland and is intended to be a high level overview of structure and processes of the risk management model.

Social Security Scotland will face risks to its strategic objectives, operational risks and risks associated with the protection of its people, property and reputation. The detail will be provided in the Risk and Issue Strategy Document.

Risk Framework-Overview

The risk framework consists of:

- Risk Identification - building a profile of risk that threatens the delivery of objectives, operations, people, property and reputation.

- Risk Analysis - prioritises risks to allow the right people and actions to be maximised; the priority would be re-analysed as the risk escalates.

- Risk Evaluation - captures the impact of the risk and how likely the risk is to occur.

- Risk Treatment - actions and controls are developed and applied to mitigate the risk.

- Communication and consultation - sharing and discussing risks with the right people to understand what threatens the delivery of objectives.

- Monitoring and review - the on-going management of risk as required by the impact and the likelihood of the risk to occur.

- Recording and reporting - providing assurance of the management of risk.

Figure 1 below is a diagram of the framework:

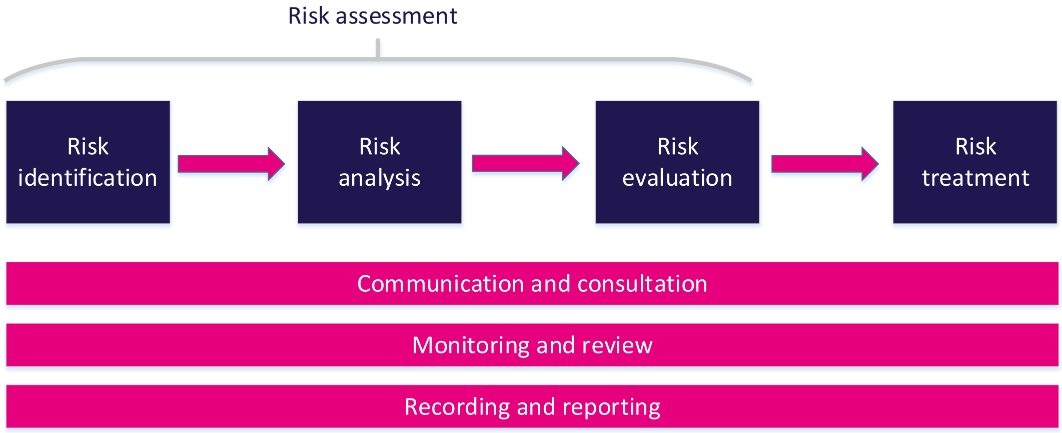

Figure 1- Risk Assessment and Reporting

More information on each section is detailed below.

Risk Framework-Details

As shown in Figure 1 (above) the Risk Framework follows the following stages. Each stage should be seen as one part of the whole process, with continuous improvement applied to assess each risk (specifically identification, analysis and evaluation).

Risk Identification

When identifying a risk consider what is the perceived threat (objective, reputation, people and places etc.). Details need to be captured on a risk log to support on-going assessment of the risks.

Risk Analysis

Once the risk has been identified consideration should be given to what type of threat it is (resource, financial, reputational, operational etc.) and consideration to who is best placed to manage the risk. Attention is to be given to how willing Social Security Scotland is to accepting this type of risk, or if there are opportunities available within the risk.

Risk Evaluation

Risk is scored based on the potential impact to an objective and how likely that impact is to happen. A target risk score is set at the lowest possible level of control that would be acceptable should the risk occur.

Risk Treatment

Consideration is given to how the risk is to be controlled. Controls (mitigations) can:

- Prevent the risk from occurring (pre-event controls);
- Manage the risk once it occurs (post-event controls).

Communication and consultation

Communication is intended to facilitate a common awareness and understanding of risk. To support risk-informed decision making, consultation involves obtaining feedback and information about risks.

Communication and consultation of risk within Social Security Scotland is intended to:

- Provide a regular update to the Executive Team, Audit Assurance Committee and Executive Advisory Board about the status of the risks threatening the strategic objectives
- Ensure that appropriate information is available to allow governance and risk assurance
- Facilitate holistic risk management by engagement with risk owners and risk action owners at all levels of the organisation
- Draw upon the risk management expertise within the organisation

Monitoring and review

Regular review of each risk should be undertaken to monitor the risk. Risks will be reviewed as follows:

Review Forum	Reporting Period
Director General's Communities Assurance	Quarterly
Executive Advisory Board	Semi-annually
Audit and Assurance Committee	Quarterly
Chief Executive and Executive Team	Monthly
Risk Review Group	Monthly
Divisional Risk Review Boards	Monthly
Project Management Office	Monthly

At Branch level risks should be reviewed regularly as a standing agenda item at regular meetings; Branch is used here to define a level of organisation below Division.

Recording and reporting

It is vital that risk logs and registers are set up to capture the information and controls. This supports visibility within Social Security Scotland and allows it to share this information with stakeholders to support our work.

Escalation and De-escalation of Risk

The escalation route of risk is based on the area and level of impact (cumulative or otherwise) of the risk.

Figure 2 (below) shows the layers of risk registers and logs and how they interact. They escalate and de-escalate through these layers.

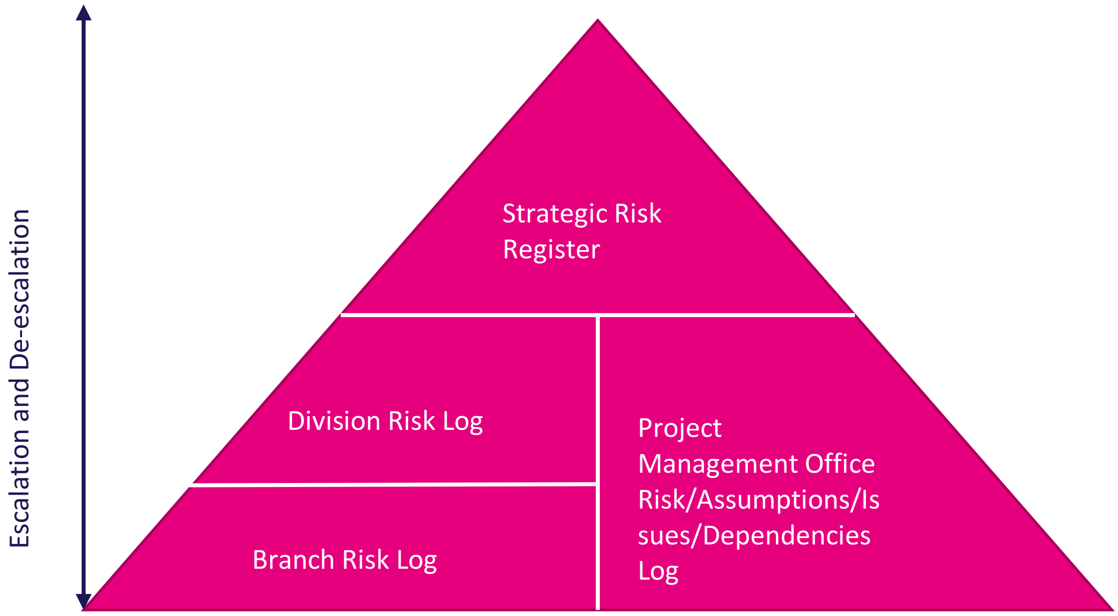
Escalation and De-escalation
Strategic Risk Register
Division Risk Log
Branch Risk Log
Project Management Office Risk/Assumptions/Issues/Dependencies Log

Figure 2 – Risk Register & Risk Log Levels for escalation

As shown in Figure 2 above there is an order of risk within Social Security Scotland with risks moving readily from Branch to Strategic level; likewise risk can be de-escalated back down the order as they become more controlled; for example, a risk that can no longer be managed at Branch level would be escalated to Divisional level following assessment and discussion with those involved in the management of that risk.

If the risk cannot be controlled at Divisional level, or the impacts of the risk reach beyond the control of a single Division it would be assessed again and presented for acceptance on to the Strategic Risk Register.

The process is followed for de-escalation whereby the risk would be assessed and decisions would be made to determine which area of the organisation will manage the risk. It should be noted that if a risk is determined to be of high enough threat on the initial assessment then it can be escalated straight to the strategic register.

Guidance for criteria for escalation and de-escalation of risks will be provided within the Risk and Issue Strategy.

During **Monitoring and Review** it may be established that a risk threatens more than a single area, or it threatens a strategic objective. A full analysis should be undertaken, with support from the Risk Management Function, where it is determined that the threat has increased or decreased. The risk is then presented to the suitable Senior Officer for approval for escalation or de-escalation.

Roles and Responsibilities

Responsibility for the Risk Management Framework is delegated to the Risk Management Function by the Accountable Officer. The Executive Team under the leadership of the Chief Executive is responsible for implementing the strategy, culture, people, processes, technology and structures which constitute the Risk Management Framework.

Governance of strategic risks is overseen by the Risk Review Group, the Chair is the Deputy Director for Finance and Corporate Services Division. The Risk Review Group membership includes senior staff from each Division within Social Security Scotland and Social Security Programme risk colleagues.

The Risk Review Group provides an objective perspective on risk and assurance and increases the understanding of the impact of risk and issues across Social Security Scotland. It provides the forum to examine and accept escalating risks on to the Strategic Risk Register. The Group are also active participants in the development of the risk and issue management strategy.

As Accountable Officer, the Chief Executive attends the Director General's Network Assurance Meeting on a quarterly basis to provide assurance that risk is being managed within Social Security Scotland and to focus on any key threats currently facing the organisation.

The Audit and Assurance Committee supports this work by providing assurance that the risk management process works effectively.

The Executive Advisory Body considers overarching strategy, direction, governance and acts as a critical friend by providing constructive challenge to the Chief Executive and his leadership team.

The Risk Management Function is responsible for the secretariat function for the Risk Review Group and coordinates the updates for the Strategic Risk Register; as part of this the Risk Management Function provide a risk practitioner role for guidance and support during risk and issue assessment.

The Risk Management Function also helps to establish risk logs, action plans, and deliver awareness on risk to those who need it. It provides updates for the Executive Advisory Body, Audit Assurance Committee and the Programme Risk Review Panel. It will also respond to any Parliamentary Questions and Freedom of Information requests on how we manage risk.

Each Division is responsible for the governance of its own risks and maintains its own divisional risk log. Each Division has a Business Support Team that has responsibility for coordination of that log.

Similarly, each Branch is responsible for the governance of its own risk and the coordination of its risk log. This is generally overseen by a senior manager

Project risks are recorded in project risk registers and managed by project team members. These risks are then collated by the Project Management Office team that works closely with the Risk Management Function and our Scottish Government colleagues in Programme to address any risks with new projects to be delivered to and by Social Security Scotland.

Programme risk is managed by Social Security Programme and shared with Social Security Scotland Project Management Office and Risk Management Function.

Risk and Issue Management Strategy

A new version of the Risk and Issue Management Strategy is being developed and will be made available in due course.

The strategy will encompass the structure and procedures for managing risks and issues within Social Security Scotland.

If you have any questions please contact the Risk Team here.