



## FOOD STANDARDS SCOTLAND

### RISK MANAGEMENT POLICY and Guidance

DATE OF ISSUE:	2022	
REVISION DATE:	30/01/2022	
VERSION NUMBER:	4	
DOCUMENT LOCATION:		
NUMBER OF PAGES:	28	
Author	NAME:	Ruth Dewar
	POSITION/ROLE:	Programme Management Officer
	SIGNATURE:	
Approver	NAME:	Garry McEwan
	POSITION/ROLE:	Head of Governance and Infrastructure
	SIGNATURE:	

## Version History

Version no.	Description of Changes
1	<b>Creation of FSS Risk Management Policy and Guidance.</b>
2	<b>Updated with revised saltire links to SG Risk Guidance and Principles.</b>
3	<b>Minor updates to narrative.</b>
4	<b>Minor updates to narrative, update to risk tolerance statement, re-alignment with current SG principles and inclusion of new risk template Annex</b>
5	<b>Updates following Strategic Risk Management Forum review</b>

INTRODUCTION .....	4
CORPORATE STATEMENT ON RISK.....	4
RISK APPETITE IN FSS.....	5
FSS RISK FRAMEWORK .....	9
CLARIFYING OBJECTIVES .....	10
RISK IDENTIFICATION .....	11
RISK ASSESSMENT.....	13
ADDRESSING RISK .....	16
INTEGRATED ASSURANCE.....	18
PURPOSE.....	18
PRINCIPLES.....	18
MANAGEMENT ASSURANCE .....	19
REVIEWING AND REPORTING RISKS.....	19
RISK ESCALATION .....	21
ROLES AND RESPONSIBILITIES.....	23
REVIEW OF RISK MANAGEMENT POLICY AND GUIDANCE .....	24
FURTHER GUIDANCE.....	24
ANNEX A – THREE LINES OF DEFENCE GOVERNANCE MODEL IN FSS .....	25
ANNEX B – ESCALATION PROCESS.....	26
ANNEX C – MODEL LEVEL 1 RISK REGISTER .....	27
ANNEX D – MODEL LEVEL 2 AND LEVEL 3 RISK REGISTERS.....	28

## INTRODUCTION

The aim of this document is to detail how and why Food Standards Scotland (FSS) carries out risk management, to lay out the roles and responsibilities across the organisation and to establish the process and techniques FSS utilise to support risk management in accordance with the principles laid out in the FSS risk policy statement.

## CORPORATE STATEMENT ON RISK

FSS's primary concern is consumer protection through making sure food is safe to eat, ensuring consumers know what they are eating and improving nutrition. With that in mind, our vision is to deliver a food and drink environment in Scotland that benefits, protects, and is trusted by consumers. By undertaking effective risk management, we will better manage the successful delivery of our objectives by:

- Reducing the possibility our objectives are jeopardised by unforeseen events through constraining threats to an acceptable level.
- Increasing confidence in achieving our desired outcomes.
- Recognising and taking informed decisions to manage and exploit opportunities that may offer an improved way of achieving objectives.
- Providing reasonable assurance to the FSS Board that we are managing risks as part of our internal controls.

Within FSS we shall operate a risk register with discretion at a fourth (project/programme) level to manage our risks accordingly:

- **Level 1** – The strategic risk register outlines strategic risks to the organisation as outlined in the FSS Corporate Plan, this will be jointly owned by the Executive Leadership Team (executive) and the board (non-executive). The Executive Leadership Team will be responsible for managing risks identified on the strategic risk register on behalf of the organisation.
- **Level 2** – Directorate Leadership Team risk register covers the tactical and operational risks faced at an Directorate Leadership Team level that will impact the delivery of the corporate plan.
- **Level 3** – Risk registers covering the tactical and operational risks faced in delivering the FSS key programmes of work and the essential core activities (ECA), both of which seek to deliver the strategic outcomes and corporate plan objectives of FSS.

The management and accountability of programme risk registers is with the senior responsible owner (SRO) with support from the programme manager and the Programme Management Office (PMO).

The management and accountability of ECA risk registers is with the relevant FSS Directors in addition to the three tiers of risk register.

- **PROJECT** – Risk registers may be developed and established to monitor risks to the delivery of specific projects or pieces of work should it be considered that the nature of the work requires it. Project managers will be responsible for the project risk registers with support from the PMO.

## **RISK APPETITE IN FSS**

Our risk appetite, detailed in the table below, reflects our overall strategy, corporate plan, and stakeholder expectations and as part of FSS governance the board has considered its risk appetite with regards to the successful delivery of the FSS strategy.

Public Health / Consumer Protection	<p><b>Averse</b> to material risks that have potentially significant impact on public health</p> <p><b>Cautious</b> where there is uncertainty around the balance of risks and benefits for public health or other consumer interests</p> <p><b>Open</b> to new approaches and partnerships with the potential to enhance public health/consumer protection or to improve dietary health</p> <p><b>Hungry</b> for innovative ways of improving the Scottish diet and reducing risks to the food chain</p>	   
Policy / Legal / Regulation / Enforcement	<p><b>Averse</b> to approaches that fall short of legal requirements</p> <p><b>Open</b> to policy/regulatory approaches that are evidence based, with the potential to produce the best outcomes in Scottish-specific circumstances</p> <p><b>Open</b> to pursuing innovative approaches for implementing regulatory standards where analysis indicates potential for significantly improved compliance</p> <p><b>Hungry</b> for policy approaches that combat the food-related effects of inequalities.</p> <p><b>Hungry</b> to apply the principles of better regulation, applying regulatory approaches which minimise burdens on businesses where appropriate</p>	    

Operational Delivery	<p><b>Averse</b> to approaches which could potentially compromise the safety or wellbeing of staff</p> <p><b>Open</b> to partnership working with the potential for improved compliance outcomes</p> <p><b>Hungry</b> to consider innovation (e.g. working practices, systems, new technologies) with the potential to deliver improved efficiency and effectiveness</p> <p><b>Hungry</b> to develop a skilled, confident and empowered workforce</p>	   
Reputation / Authority / Public Confidence	<p><b>Cautious</b> about activities which could impact on our ability to influence effectively to protect consumers</p> <p><b>Open</b> to making evidence-based decisions and recommendations and influencing opinion where we are clear that the benefits for consumers outweigh the risk</p> <p><b>Open</b> to advocacy on behalf of consumers, where there is evidence to support their interests</p> <p><b>Hungry</b> to exploit communication channels which promote FSS as the trusted source of advice on food safety, standards, diet and nutrition</p>	   

Relationships / Partnerships	<p><b>Cautious</b> around our relationships with industry and Government to safeguard our independence and ensure our work prioritises consumer interests</p> <p><b>Open</b> to contributing to Scottish Government strategy for promoting sustainable economic growth within the Scottish food and drink sector and supporting future export markets, ensuring there is no conflict with our consumer protection role</p> <p><b>Open</b> to working with all partners who are able to help us in achieving our strategic goals</p> <p><b>Hungry</b> to form partnerships with the potential to influence consumers' dietary behaviour</p>	   
Financial	<p><b>Averse</b> to risks of internal fraud or corruption</p> <p><b>Minimalist</b> but willing to consider options with other financial risks if they have the potential to deliver success</p> <p><b>Open</b> with regard to new approaches which could impact on efficiency and value</p>	  
External Factors	<p><b>Minimalist</b> to risk of impact of external events; robust business continuity and incident management plans in mitigation</p>	

## FSS RISK FRAMEWORK

FSS have adopted the principles of the Scottish Government risk framework. The methodology is straightforward and aims to assist the organisation manage risk effectively, following 5 distinct phases.

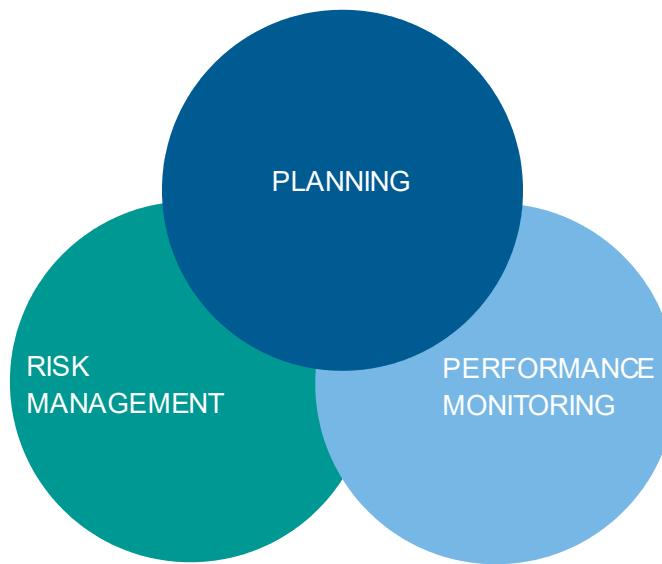
- **Clarifying objectives:** This may be established through directorate, branch or programme/project planning. There should be a direct link between what you want to achieve and the risks you are managing to make the risk environment meaningful.
- **Identifying risks:** To manage risks, you need to know what risks are faced and to undertake an evaluation – this is the first step in building a risk profile – an overview of the short, medium and long-term risks that may affect the achievement of objectives.
- **Assessing risks:** This enables the effective prioritisation of risks in relation to objectives and ensures attention is focussed on the key risks and resources are concentrated where they are most required.
- **Addressing risks:** This is the stage where actions are agreed in order to control or mitigate the risks that have been identified.
- **Reviewing and reporting risks:** This ensures new opportunities and threats, or changes to existing risks, are managed. Reporting changes helps to raise awareness and coordinate responses to key risks.



## CLARIFYING OBJECTIVES

The first phase of the risk management framework is to understand the objectives that you are trying to achieve. This could be at an FSS, directorate, divisional, branch, programme or project level.

This will then be the focus of any risk management information. A risk is anything that can impede or enhance your ability to meet current or future objectives. Through this process FSS are aiming to improve our performance through better informed decision making and planning. Risk identification needs to be undertaken with a clear strategy and clarity of purpose and is an important part of managing priorities effectively.



The aim here is to ensure a direct link between risk management and the aims and objectives, whether it be organisational or at an individual project level. It allows focus to be achieved on relevant risks that may present an opportunity or threat to the stated goals or deliverables.

At an organisational level, this should be consistent with the FSS business planning process:

- **Delivery Objectives** (“What”) – contribution to the FSS statutory responsibilities and Strategy
- **Business Objectives** (“How”) – proposals within the FSS Corporate Plan that will deliver the business Strategy
- **Risk Management** (“What If”) – the approach to managing risk within FSS as outlined in this policy guidance

## RISK IDENTIFICATION

Risk is the uncertainty that may impact, either positively or negatively, on the achievement of objectives.

Ensuring all of your risks follow the same format will support review and moderation and make clear the focus of a particular risk to anyone who reads your register. Following this guide should also make it easier for you to determine the right, and most effective, mitigations and controls for your risks.

In describing a risk for monitoring and reporting it is helpful to consider cause, event and effect when defining a risk. This can focus the discussion on what action is required to manage a risk effectively.

To represent the cause, event and effect, risk descriptions can be seen as a combination of 'if', 'then' and "resulting in" statements.

- **A Risk Cause – “IF” statement**
- **A Risk Event – “THEN” statement**
- **A Risk Effect – “RESULTING IN” statement**

Strategic risks will be identified by the Executive Leadership Team/FSS Board in line with the 5 risk areas recognised within the FSS strategy as being a key risk to the delivery of the strategy, or will be adopted following escalation from directorate or programme/project risk registers.

It is useful to have a systematic process in place to help identify risk and give assurances that a complete risk profile is articulated. Within FSS, two simple techniques are recommended that provide a wide scan of areas that may affect objectives.

## PESTLES

CATEGORY	EXAMPLES
Political	Changes in SG policy, stakeholder relationships, ministerial changes, wider political changes – EU exit and UK position.
Economic	Budget constraints, effect on economy on food and consumer behaviours, sustainability.
Social	Demographic influence on FSS policy, trust of consumers, staff implications, changes in consumer engagement methods.
Technological	Cost and efficiency of IT solutions, change in technology and obsolescence, technical competence of organisation.
Legal	EU requirements, procurement processes around official controls and other key contracts, accounting rules, legal challenge on FSS policies/proposals.
Environmental	Changing environmental standards, changes to consumer shopping habits, staff changes and loss of expertise, change in official control delivery methods.
Security	Physical assets, information security and data protection.

## SWOT

SWOT analysis can also be applied to risk identification and specific pieces of work, focussing on:

**Strengths:** Internal attributes that are helpful to achieving an objective.

**Weaknesses:** Internal attributes that are harmful to achieving an objective.

**Opportunities:** External conditions that are helpful to achieving an objective.

**Threats:** External conditions that are harmful to achieving an objective.

EXAMPLES:

Strengths	Staff experience, management support
Weaknesses	Communications channels, timescales
Opportunities	Stakeholder relationships, IT developments
Threats	Geographic spread, current culture

## RISK ASSESSMENT

It is important to clearly establish a structured process in which both likelihood and impact are considered for each risk and that the assessment of risk is recorded in a way that facilitates monitoring and prioritisation. A risk in FSS is assessed on the combination of the consequences of an event (impact) and the probability (likelihood). The table below provides a guide to risk levels and how they should be recorded in the FSS risk register template.

FSS risk registers require the risk owner to identify and record a 'target' risk score as well as the 'current' risk score. The 'target' risk score is a score which the risk owner has determined as being tolerable after having undertaken the process of addressing the risk and considered the actions to be taken and the FSS appetite for the risk. The risk owner should consider the board's agreed risk appetite statement when determining the 'target' risk score and the resulting action required to mitigate the risk to the desired level of tolerance.

The risk owner shall carry out such mitigating actions as necessary to reduce the 'current' score to that of the 'target' score. The risk owner must then consider if any further actions to reduce the risk score below that of the target (or tolerable) score are appropriate or necessary having considered the time, effort, and cost of implementing such further actions.

*For example, where a risk has been reduced from a current score of 100 (very high) to a tolerable target score of 20 (medium), the risk owner would then consider whether actions to reduce further to a score of 10 (medium) are necessary or cost effective.*

All agreed target scores must be reviewed at least annually to ensure they remain aligned with the current risk appetite. Changes in risk appetite may require an adjusted target score either higher or lower.

**IMPACT** – The estimated effect of the risk on the objective or strategic outcome in question. This is focussed on scale, scope and resource implications, as well as the risk appetite of FSS.

IMPACT	CRITERIA
VERY HIGH – 50	Destructive and unacceptable impact on corporate plan objectives or strategic outcomes that would result in a major change to overall approach. Potentially large resource consequences (> £100k) that outweigh current operational circumstances.
HIGH – 25	Significant and unacceptable impact on corporate plan objectives or strategic outcomes that would require a material change to critical approach/procedure/process. Resource implications would be challenging to absorb (£50-100k) within current operational circumstances.
MEDIUM – 10	Moderate impact on corporate plan objectives or strategic outcomes that may require multiple changes in approach/procedure/process. Acceptable level of resource consequences (£10-50k).
LOW – 5	Minor impact on corporate plan objectives or strategic outcomes, requires little overall change in approach. Few resource consequences (£1-10k).
NEGLIGIBLE – 1	No real impact on achieving corporate plan objectives or strategic outcomes. Financial impact < £1k.

**LIKELIHOOD** – This is the estimated chance of the risk occurring and is focussed on probability.

LIKELIHOOD	CRITERIA
VERY HIGH – 5	> 75% chance of occurring – almost certain to occur
HIGH – 4	51-75% chance of occurring – more likely to occur than not
MEDIUM – 3	26-50% chance of occurring – fairly likely to occur
LOW – 2	6-25% chance of occurring – unlikely to occur
RARE – 1	1-5% chance of occurring – extremely unlikely to occur

Most risks are time based and are not constant and estimating the timing of when a risk may occur is sometimes called ‘proximity’. Considering this should inform a judgement on the impact or likelihood of a risk and the timing of any response.

The tables below provide a guide, in line with the SG risk management methodology, to the overall risk level based on multiplying the assessment of the impact and likelihood of a risk. This then informs the risk scores recorded on the FSS risk register template.

**ASSESSING THE IMPACT AND LIKELIHOOD OF A RISK (5X5 MATRIX):**

Impact	Multiplier	50	100	150	200	250
Very High	50	50	100	150	200	250
High	25	25	50	75	100	125
Medium	10	10	20	30	40	50
Low	5	5	10	15	20	25
Negligible	1	1	2	3	4	5
Multiplier		1	2	3	4	5
Likelihood		Rare	Low	Medium	High	Very High

**ASSESSING THE OVERALL RISK LEVEL:**

Risk Level	Score	Risk Level Description
Very High	100-250	<b>Rating:</b> Unacceptable level of risk exposure that requires immediate mitigating action. <b>Reporting:</b> Report the risk to Executive Leadership Team/audit committee/board.
High	40-75	<b>Rating:</b> Unacceptable level of risk which requires controls to be put in place to reduce exposure. <b>Reporting:</b> A decision should be taken as to whether risks recorded as high should be escalated. Scores between 40 and 60 would not usually be escalated where scores between 61 and 75 should be given careful consideration.
Medium	10-30	<b>Rating:</b> Acceptable level of risk exposure subject to regular active monitoring. <b>Reporting:</b> At directorate level.
Low	1-5	<b>Rating:</b> acceptable level of risk subject to regular passive monitoring. <b>Reporting:</b> at directorate level. consideration should be given as to whether risks recorded as low are still extant.

As outlined above, once risks have been assessed the risk priorities for FSS will emerge. The less acceptable the exposure in respect of a risk, the higher the priority which should be given to addressing it. The highest priority risks (e.g., key risks) should be given regular attention at the highest level of the organisation.

## ADDRESSING RISK

Once risks have been identified and assessed the next stage is to decide what action needs to be taken to address the highlighted risks. The purpose of addressing risks is to turn uncertainty to FSS's benefit by constraining threats and taking advantage of opportunities. There are 5 key aspects of addressing risk, depending on the kind of challenge they present according to how likely they are to occur, and the impact if they did occur.

- **Tolerate:** For unavoidable risks the exposure may be tolerable without any further action being taken, or so remote as to take mitigating action may be disproportionate to the potential benefit gained.
- **Treat:** For risks that can be reduced or eliminated, by prevention or other control action (new systems, revision of processes etc.). By far the greatest number of risks will be treated in this way.
- **Transfer:** Where another party can take on some, or all of the risk, more economically or more effectively (e.g. sharing risk with a contractor). Some risks are not fully transferable. It is generally not possible to transfer reputational risk even though the delivery of a service is contracted out.
- **Terminate:** For risks no longer deemed tolerable, and where exit is possible (e.g. elements of first class travel arrangements). This option is severely limited in Government but can be particularly important in project management if it becomes clear that the projected cost/benefit is in jeopardy.
- **Take the opportunity:** This option should be considered whenever tolerating, treating, or transferring a risk and focusses on managed risk taking. Judgement should be taken on the level of exposure which is considered tolerable should it be realised.

When considering the option of ‘treat’ in addressing risk the following approach should be undertaken when designing control mechanisms to mitigate the risk:

- **Preventative controls:** Designed to limit the possibility of an undesirable outcome being realised. The more important an undesirable outcome should not arise, the more important it becomes to implement appropriate preventative controls. For example – separation of duty or limitation of action to authorised persons.
- **Corrective controls:** Designed to correct undesirable outcomes which have been realised. They provide a route to achieve some recovery against loss or damage. For example – design of contract terms to recover an overpayment or contingency planning as this allows an organisation to plan for business continuity or recovery after events which they could not control.
- **Directive controls:** Designed to ensure that a particular outcome is achieved. They are particularly important when it is critical an undesirable event is avoided. For example – a requirement for protective clothing to be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.
- **Detective controls:** Designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, after the event so they are only appropriate when it is possible to accept the loss or damage. For example – stock or asset checks which detect removal without permission, post implementation reviews which detect lessons learnt, and monitoring activities which detect changes that should be responded to.

In designing controls, it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of human life) it is normally sufficient to design controls to give a reasonable assurance of confining likely loss within the risk appetite of FSS. The purpose of control is to constrain risk rather than to eliminate it.

Where the option to ‘treat’ the risk, by implementing one or more of the above controls, the risk owner will be required to re-score the risk, taking account of the degree to which the designed controls have constrained/reduced the risk.

*For example, a designed control may mitigate the risk by reduction of the likelihood that a risk event will occur and/or reduction of the impact/effect of a risk event if it does occur. If either the likelihood or impact/effect (or both) is reduced, then the overall score will be reduced, and this must be recorded for comparison and assessment of the control.*

## **INTEGRATED ASSURANCE**

We aim to provide consistent, co-ordinated, structured, and reasonable assurance over key organisational risks and controls put in place to ensure we achieve our objectives.

## **PURPOSE**

The assurance process will:

- Provide timely and reliable information on the effectiveness of the management of strategic risks and significant control issues.
- Provide a mechanism for co-ordinating and communicating the provision of reasonable assurance over key risks and controls.
- Facilitate the escalation of risk and control issues requiring visibility and attention by ELT, by providing a cohesive and comprehensive view of assurance across the risk environment.
- Provide an opportunity to identify gaps in assurance needs that are vital to FSS, and to address them in a timely, efficient, and effective manner.
- Demonstrate “at a glance” where controls are working as intended and where they can be strengthened.
- Raise FSS understanding of risk and strengthen accountability and clarity of ownership of controls and assurance, avoiding duplication or overlap. Provide consistent and appropriately detailed supporting evidence for the CEO’s annual governance statement in the annual report and accounts.
- Providing greater oversight of assurance activities for the board/audit & risk committee (ARC) in line with the FSS risk appetite.
- Assist with the internal audit planning process.

## **PRINCIPLES**

- Assurance uses the ‘three lines of defence’ governance model as its basis (**see ANNEX A** for further information). This model is a useful way to picture, and gain understanding of, assurance provision within an organisation. The first line of defence is management assurance and applies to business units or operational areas. It covers day to day risk management and application of internal controls. The second line is the corporate oversight level which oversees and challenges risk management and is responsible for the development of the risk management framework. The third line is led by internal

audit but includes external reviews and brings an independent objective perspective to assurance.

- The intention is to gain “reasonable assurance” that the key risks are being controlled as intended – this means using FSS’s key objectives, scope and stated risk appetite to focus on key accountabilities, key risks and key controls.

## MANAGEMENT ASSURANCE

The framework reflects best practice as outlined in the [internal control checklist](#) section of the [Scottish public finance manual](#).

There are eleven assurance areas in the risk management, business planning, project management, financial management, fraud, procurement, human resources, equality, information, health and safety and compliance. There are two additional sections (review and other) within the framework which are included within the internal controls checklist which supplement the eleven assurance areas. These sections allow branch heads to raise any general issues around effectiveness of controls and highlight areas where additional action has been taken to improve and validate any internal controls within their areas. All of the identified areas should be considered when thinking about assurances in place linked to identified risks within the risk register.

## REVIEWING AND REPORTING RISKS

The management of risk, including risk registers (see Annex A & B), should be reviewed regularly to monitor whether or not the risk profile of FSS is changing, to gain assurance that risk management is effective, and to identify when further action is necessary. FSS currently mandates the following suite of risk registers

- Level 1 - Strategic register
- Level 2 – Directorate Leadership Group (DLG) register
- Level 3 - Directorate registers (x2) / programme registers (x2)

Within FSS, reviews will be undertaken as a minimum:

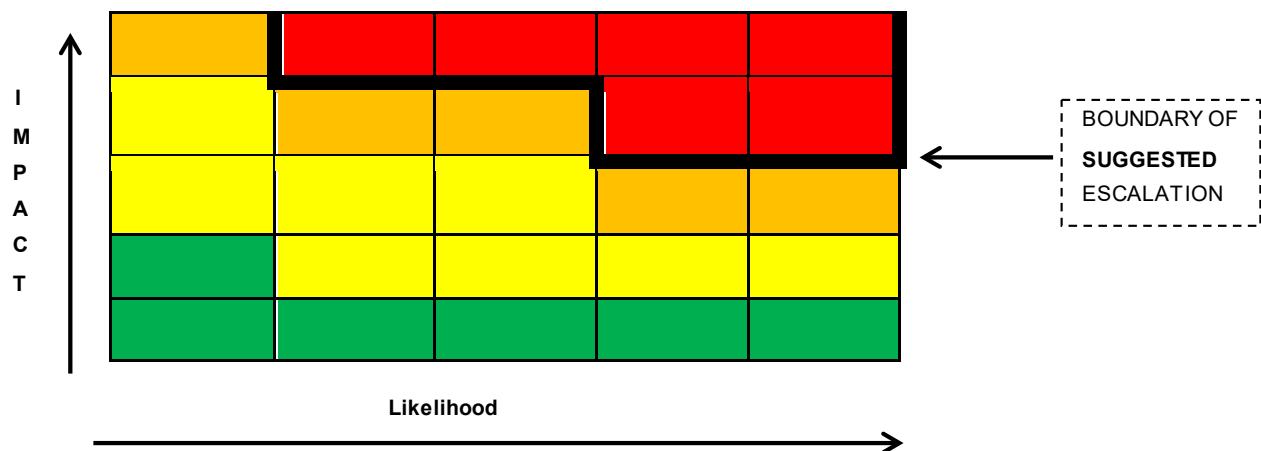
- The level 1 risk register will be reviewed at a monthly Strategic Risk Management Forum led by the Executive Leadership Team with attendance from division heads or appointed delegate. Level 2 and 3 (ECA) risk registers will be reviewed on a monthly basis at DLG and director led meetings as required. All risks rated high or very high will be reviewed in detail and action taken to mitigate risks further, as required. cross directorate challenge is welcomed at level 3 should it be appropriate.

- Level 3 (programme) risk registers will be reviewed in accordance with the individual reporting arrangements agreed by the relevant programme board and in accordance with the reporting timetable set out by the PMO.
- The strategic risk register will also be reviewed by the board annually or by exception, through escalation by DLG and the audit and risk committee, as required.
- The strategic risk register will be reviewed quarterly by the FSS ARC. This will form the basis of a report that will comprise of a summary of all risks rated very high and a copy of the latest version of the strategic risk register. Any red risks on the level 2 DLG risk register shall also be reported to the committee.
- Discretionary project risk registers will be reviewed in accordance with the individual reporting arrangements agreed by the relevant project manager and in accordance with the reporting arrangements set out by the programme manager or branch with support from the PMO.

## RISK ESCALATION

When a risk reaches a level whereby the risk owner can implement no further controls or solutions, the risk must be escalated (see **ANNEX B** for further information).

The boundary for suggested escalation within FSS is outlined below. If the risk owner/director deems the risk to be of corporate significance, or beyond their delegated tolerance, they can however escalate a risk to the SRMF if they are deemed critical or effect FSS as a whole, e.g., if a programme 'amber risk' is identified which has the potential to negatively impact on FSS' s reputation. They will then be considered as corporate risks and will be under ELT management and control.



The FSS policy for risk escalation is that all risks rated very high, or red should be discussed and considered for escalation to the next level in the risk management chain. Risks that are not rated very high or red, but have been highlighted as having the potential to have a wider impact within FSS, or where the scoring gap between the current risk score and target (or tolerable) risk score are considerable, should also be discussed. The FSS risk escalation hierarchy is outlined below and is designed to provide effective support and challenge in managing FSS risks.

**FSS BOARD** – Consideration of appropriate risks on the Level 1 strategic risk register following discussion and review with ARC.

**FSS AUDIT AND RISK COMMITTEE** – Consideration of strategic risk register and all **VERY HIGH** or **RED** risks reported on DLG risk register following DLG discussions.

**DIRECTORATE LEADERSHIP GROUP** – Consideration of Level 2 risks and any **VERY HIGH** or **RED** risks on Level 3 or programme risk registers.

**PROGRAMME BOARD** – Consideration of all programme & project-level **RED** risks or those identified as impacting on the other programmes or the strategy.

**DIRECTORATE** – Consideration of all Level 3 risks on Directorate registers and through role as SRO in relation to programme or project risk registers.

The following diagram shows the risk owner how and where to escalate and/or communicate very high/red risks or risks which may impact on other programmes, projects, or strategic objectives.

#### STRATEGIC & PROGRAMME LEVEL RISKS

**COMMUNICATED** to this level where they could affect project objectives. Risks relating to individual projects should be communicated to other projects & operations where appropriate.

PROJECT BOARD/OPERATIONAL LEVEL

PROGRAMME BOARD LEVEL

STRATEGIC (FSS BOARD/ARC/ELT LEVEL)

**ESCALATED** against set criteria where they exceed agreed tolerances, such as an unacceptable exposure to risk, if they fall outside certain limits, or if they could affect PROGRAMME objectives.

PROJECT & OPERATIONAL LEVEL RISKS

**ESCALATED** to this level against set criteria where they exceed agreed tolerances – such as an unacceptable exposure to risk, if they fall outside certain limits, or if they could affect strategic objectives.

PROGRAMME, PROJECT & OPERATIONAL LEVEL RISKS

## ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
<b>FSS Board</b>	Overall responsibility for the FSS system of internal control and ensuring that an effective risk management system is in place.
<b>Audit And Risk Committee</b>	Advise and provide assurance to the board on FSS's arrangements for risk management, through constructive challenge and review.
<b>Accountable Officer</b>	Responsible for ensuring and implementing effective risk management processes within FSS and programmes of activity. Ensure there is comprehensive risk reporting arrangements for their area of accountability.
<b>Strategic Risk Management Forum</b>	Review level 1 risks and individual escalated risks. Take appropriate action to mitigate risks. Review level 1 risks and new high-level risks bi-monthly and advise as to whether contingency plan is required.
<b>Directorate Leadership Group</b>	Manage level 2 risks. Escalate corporate and very high rated risks (beyond their own tolerance) to the SRMF (level 1 risk register).
<b>Head Of Governance and Infrastructure</b>	Develop, operate, monitor, and report on FSS risk management system embed risk aware culture within FSS through appropriate learning and development activities. Provide guidance and support to branch, project, programme, directorate, and senior management on risk management methodology within FSS.
<b>Division Heads</b>	Identify, evaluate, and manage risks to the delivery of branch or corporate plan objectives.
<b>Programme Management Office</b>	Manage and monitor risk registers on behalf of programme managers. Identify common risks across programmes or projects so they can be managed more efficiently or escalated. highlight increasing risks and potential new risks to programme manager.
<b>Programme Boards</b>	Monitor and review red high-level risks to the delivery of programme or project objectives Escalate to ELT (level 1 risk register) as necessary.
<b>Senior Responsible Owners (SRO)</b>	Accountable for the programme risk register and ensures risk management activities are operating effectively and that key risks are being dealt with at the appropriate senior level. Monitor and review all risks to the delivery of programme or project objectives. Review and manage high level programme/project risks and escalate to Executive Leadership Team (level 1 risk register) as necessary.
<b>Programme Managers</b>	Ensure risk management activities are being carried out through the programme and respective projects. Identify, evaluate and manage risks to the delivery of programmes and projects. Escalate risks to SRO/programme board as necessary.
<b>All Staff</b>	Take ownership of individual branch and project risks where appropriate. Be responsible for managing risks as an integral part of the branch.

## **REVIEW OF RISK MANAGEMENT POLICY AND GUIDANCE**

To ensure it remains fit for purpose, this policy and associated documents will be reviewed, as a minimum, on an annual basis.

## **FURTHER GUIDANCE**

Further guidance on the FSS risk management policy can be sought from the Head of Governance and Infrastructure or additional information and supporting documentation on risk management within Government can be found:

HM treasury orange book -

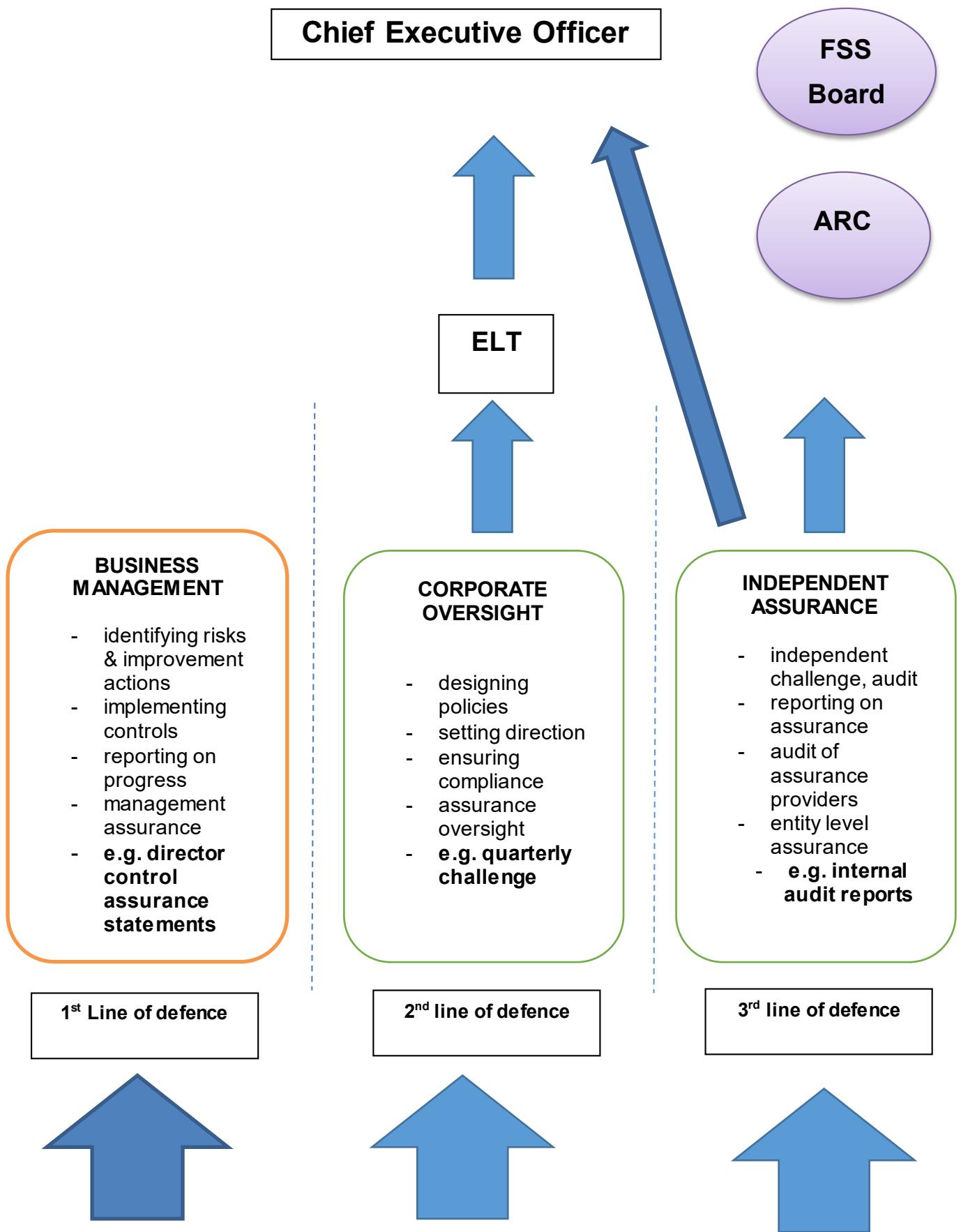
[https://www.gov.UK/government/uploads/system/uploads/attachment\\_data/file/220647/orange\\_book.pdf](https://www.gov.UK/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf)

Scottish Government risk management –

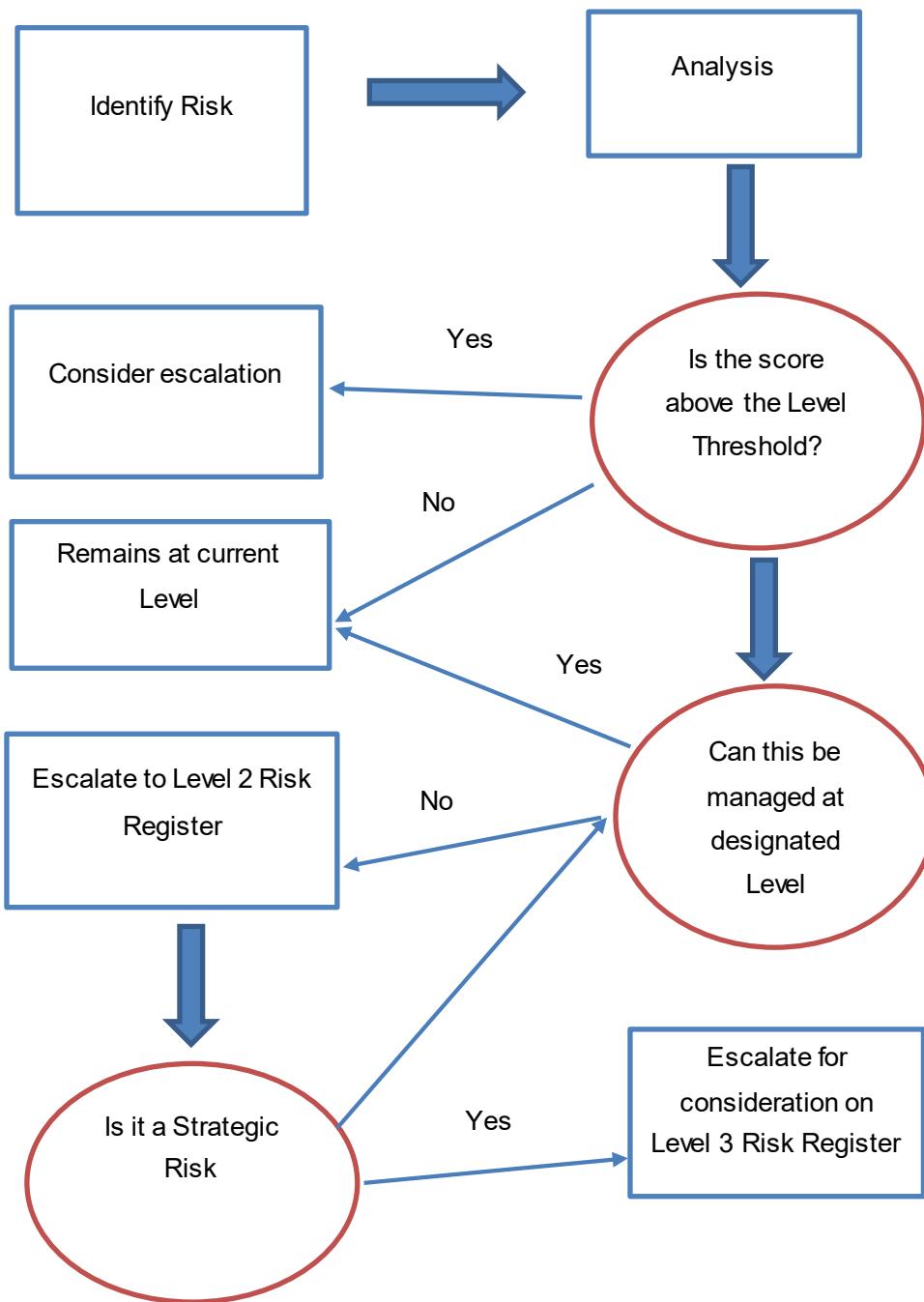
[corporate governance](#) Scottish public finance manual –

[Scottish public finance manual - gov.scot \(www.gov.scot\)](#)

## ANNEX A – THREE LINES OF DEFENCE GOVERNANCE MODEL IN FSS



## ANNEX B – ESCALATION PROCESS



## ANNEX C – MODEL LEVEL 1 RISK REGISTER

Risk No	Executive Lead	Version Date:
Risk Title		Risk Description Event:. Cause: Effect:
Strategic Objective(s)		Strategic Goals

Current Risk					Target Risk		
likelihood	Impact	Score	Trend	Proximity	likelihood	Impact	Score
CONTROLS IN PLACE							
Quarter							
Goal	Mitigating Actions					% Complete	Status

Update on Corporate Plan Progress/Reasons for Delay	
Goal	
Corrective Actions	
Goal	
Corrective Actions	

## ANNEX D – MODEL LEVEL 2 AND LEVEL 3 RISK REGISTERS

Risk No	Directorate	Risk Owner	Risk Title	Risk Description Include: Event - Cause - Effect	Link to Strategic Outcome	Controls in Place (To be aligned with Internal controls)	Assurance Three Lines of Defence			Gaps in Assurance	CURRENT Risk Impact & Likelihood			Trend	Proximity	Mitigation Actions Planned & Date of Delivery	TARGET Risk Impact & Likelihood		
							1st Line	2nd Line	3rd Line		Likelihood	Impact	CURRENT Risk Score				Likelihood	Impact	TARGET Risk Score